УДК 510.7
ББК 22.12
У 77

Успенский В. А., Верещагин Н. К., Плиско В. Е. **Вводный курс математической логики.** — 2-е изд. — М.: ФИЗМАТЛИТ, 2004. — 128 с. — ISBN 5-9221-0278-8.

В учебном пособии содержится материал основного курса «Введение в математическую логику», читаемого на механико-математическом факультете МГУ. Излагаются элементы теории множеств, основные понятия, относящиеся к семантике формализованных логико-математических языков первого порядка, исчисление предикатов и теорема о его полноте, дается введение в теорию алгоритмов и вычислимых функций.

Для студентов математических факультетов университетов, педагогических институтов, а также других вузов с углубленным изучением информатики и кибернетики.

Библиогр. 15 назв.

ISBN 5-9221-0278-8

ОГЛАВЛЕНИЕ

ГЛАВА 4
ТЕОРЕМА ГЁДЕЛЯ О ПОЛНОТЕ

ГЛАВА 5
ТЕОРИЯ АЛГОРИТМОВ

ВВЕДЕНИЕ

Логику можно определить как науку о правильных способах рассуждения, т. е. таких способах рассуждения, при которых из верных исходных положений получаются верные результаты.

Конечно, можно рассуждать и без науки о правильных рассуждениях. Однако в некоторых случаях потребность в такой науке все же возникает. В частности, такая ситуация сложилась в математике в конце XIX — начале XX вв., когда были обнаружены парадоксы в теории абстрактных множеств, разработанной Г. Кантором. Анализ парадоксов потребовал внимательного исследования рассуждений, применяемых в математике, и тем самым вызвал необходимость в развитии науки о рассуждениях, т. е. логики.

Чтобы логика могла обслуживать самую точную из наук — математику, она сама должна быть точной наукой, т. е. она должна иметь дело с точными математическими понятиями и применять точные математические методы. Такова математическая логика — наука о математических рассуждениях, пользующаяся математическими методами.

Современная математическая логика представляет собой обширный и разветвленный раздел математики. Она, конечно, полезна и для других наук, поскольку в них используются рассуждения, доказательства и т. п. В настоящее время разработаны приложения математической логики к другим разделам математики, а также к кибернетике и программированию.

Г Л А В А 1

ЭЛЕМЕНТЫ ТЕОРИИ МНОЖЕСТВ

§ 1. Основные понятия теории множеств

В начальный период развития теории множеств пользовались интуитивным понятием множества. Согласно Кантору, *множество* — это любое объединение в одно целое определенных объектов, которые называются *элементами* этого множества. Тот факт, что x есть элемент множества A, записывается так: $x \in A$. Если $x \in A$, то говорят, что A содержит x или что x принадлежит A. Если же x не является элементом множества A, пишут $x \notin A$.

Два множества A и B считаются *равными*, если они состоят из одних и тех же элементов, т. е. каждый элемент множества A принадлежит множеству B и каждый элемент множества B принадлежит множеству A. Запись $A = B$ означает, что A и B равны, а $A \neq B$ — что A и B не равны. Запись $A \subseteq B$ означает, что каждый элемент множества A является также элементом множества B; в этом случае говорят, что A является *подмножеством* множества B или что A *включено* в B. Если $A \subseteq B$ и $A \neq B$, то A называется *собственным подмножеством* B, и в этом случае пишут $A \subset B$. Множество, не содержащее элементов, называется пустым и обозначается $\varnothing$. Семейство всех подмножеств данного множества A обозначается $\mathcal{P}(A)$.

Множество, элементами которого являются данные объекты a_1, $a_2, \ldots$, обозначается $\{a_1, a_2, \ldots\}$. Например, $\{a, b\}$ есть множество с элементами a и b. Если при этом $a \neq b$, то $\{a, b\}$ называется неупорядоченной парой объектов a и b. Множество $\{a, a\}$ можно обозначить также $\{a\}$. Это одноэлементное множество с элементом a. Через $\{x \mid \Phi(x)\}$ обозначается множество таких элементов x, для которых выполняется условие $\Phi(x)$.

Множество $A \cup B = \{x \mid x \in A \text{ или } x \in B\}$ называется *объединением* множеств A и B. *Пересечением* множеств A и B называется множество $A \cap B = \{x \mid x \in A \text{ и } x \in B\}$. *Разностью* множеств A и B называется множество $A \setminus B = \{x \mid x \in A \text{ и } x \notin B\}$.

§ 2. Бинарные отношения и функции

Через $\langle a, b\rangle$ обозначается *упорядоченная пара* двух объектов a и b. Основное свойство упорядоченных пар таково: каковы бы ни были объекты a_1, a_2, b_1, b_2, равенство $\langle a_1, b_1\rangle = \langle a_2, b_2\rangle$ имеет место тогда и только тогда, когда $a_1 = a_2$ и $b_1 = b_2$. Вообще, для любого натурального числа n можно образовать кортежи длины n (или, как иногда говорят, упорядоченные n-ки) объектов $\langle a_1, \ldots, a_n\rangle$ с тем свойством, что $\langle a_1, \ldots, a_n\rangle = \langle b_1, \ldots, b_n\rangle$ тогда и только тогда, когда $a_i = b_i$ $(i = 1, \ldots, n)$.

Прямым (или *декартовым) произведением* множеств A и B называется множество $A \times B$, состоящее из всех таких упорядоченных пар $\langle a, b\rangle$, что $a \in A$ и $b \in B$. Аналогично определяется прямое произведение множеств $A_1, \ldots, A_n$ как множество, состоящее из всех таких кортежей $\langle a_1, \ldots, a_n\rangle$, что $a_1 \in A_1, \ldots, a_n \in A_n$.

Бинарным отношением между элементами множеств A и B называется любое подмножество R множества $A \times B$. Часто вместо $\langle x, y\rangle \in R$ пишут xRy. *Областью определения* бинарного отношения R называется множество δ_R, состоящее из всех таких x, что $\langle x, y\rangle \in R$ хотя бы для одного y. *Множеством значений* ρ_R бинарного отношения R называется множество всех таких y, что $\langle x, y\rangle \in R$ хотя бы для одного x. *Обратным отношением* для бинарного отношения R называется множество R^{-1}, состоящее из всех таких упорядоченных пар $\langle x, y\rangle$, что $\langle y, x\rangle \in R$. Заметим, что $\delta_{R^{-1}} = \rho_R$; $\rho_{R^{-1}} = \delta_R$. Если R_1 — отношение между элементами множеств A и B, а R_2 — отношение между элементами множеств B и C, то можно образовать *произведение* (*композицию*) отношений R_1 и R_2. Произведением $R_1 \circ R_2$ отношений R_1 и R_2 называется отношение между элементами множеств A и C, состоящее из всех пар $\langle x, z\rangle$, для которых найдется такой элемент $y \in B$, что $\langle x, y\rangle \in R_1$ и $\langle y, z\rangle \in R_2$. Например, если M — множество всех живущих или когда-либо живших мужчин на Земле, а отношение $R \subseteq M \times M$ состоит из таких пар $\langle x, y\rangle$, что x является отцом y, то R^{-1} — это отношение, состоящее из таких пар $\langle x, y\rangle$, что x является сыном y, а $R \circ R$ — отношение, состоящее из всех таких пар $\langle x, y\rangle$, что x является дедушкой y по отцовской линии.

Отношение f называется *функцией*, если из $\langle x, y\rangle \in f$ и $\langle x, z\rangle \in f$ следует $y = z$. Функция f называется функцией из A в B, если $\delta_f \subseteq A$, $\rho_f \subseteq B$; если при этом $\delta_f = A$, то пишут $f : A \to B$. Если f — функция и $\langle x, y\rangle \in f$, то обычно пишут $y = f(x)$ и называют y *значением* функции f при значении аргумента x. Если не существует такое y, что $\langle x, y\rangle \in f$, то выражение $f(x)$ считается *неопределенным*.

Среди функций из A в A выделим так называемую *тождественную функцию* $id_A = \{\langle x, x\rangle \mid x \in A\}$. Очевидно, что $id_A(x) = x$, каков бы ни был элемент $x \in A$.

Функция f называется *последовательностью*, если ее область определения — это множество натуральных чисел $\mathbb{N} = \{0, 1, 2, \dots\}$.

В случае, когда множества A и B совпадают, бинарное отношение R между элементами множеств A и B называется *бинарным отношением на множестве* A. Бинарное отношение R на множестве A называется:

рефлексивным, если $\langle x, x\rangle \in R$ для всех $x \in A$;

иррефлексивным, если $\langle x, x\rangle \notin R$ для любого $x \in A$;

симметричным, если из $\langle x, y\rangle \in R$ следует $\langle y, x\rangle \in R$;

антисимметричным, если из $\langle x, y\rangle \in R$ и $\langle y, x\rangle \in R$ следует $x = y$;

транзитивным, если из $\langle x, y\rangle \in R$ и $\langle y, z\rangle \in R$ следует $\langle x, z\rangle \in R$.

Бинарное отношение на множестве A называется *частичным упорядочением* (или *частичным порядком*), если это отношение рефлексивно, антисимметрично и транзитивно. Частичное упорядочение обычно обозначается символом $\leqslant$. Множество A с заданным на нем частичным порядком $\leqslant$ называется *частично упорядоченным* и обозначается $(A, \leqslant)$.

Бинарное отношение на множестве A называется *строгим частичным упорядочением* (или *строгим частичным порядком*), если это отношение иррефлексивно и транзитивно. Строгое частичное упорядочение обычно обозначается символом $<$. Множество A с заданным на нем строгим частичным порядком $<$ называется *строго частично упорядоченным* и обозначается $(A, <)$.

Бинарное отношение на множестве A называется *отношением эквивалентности*, если это отношение рефлексивно, симметрично и транзитивно.

Упражнения.

1. Пусть A и B — конечные множества, состоящие из m и n элементов соответственно.

а) Сколько существует бинарных отношений между элементами множеств A и B?

б) Сколько имеется функций из A и B?

2. Образуют ли бинарные отношения на множестве A группу относительно операций $\circ$ и $^{-1}$?

3. Доказать, что для любых функций $f : A \to B$ и $g : B \to C$ их композиция $f \circ g$ является функцией из A в C, причем $(f \circ g)(x) = g(f(x))$.

4. Доказать, что всякое строгое частичное упорядочение является антисимметричным.

5. Пусть $(A, \leqslant)$ — частично упорядоченное множество. Доказать, что бинарное отношение $R = \{\langle x, y\rangle \mid x \leqslant y$ и $x \neq y\}$ является строгим частичным порядком на множестве A.

6. Пусть $(A, <)$ — строго частично упорядоченное множество. Доказать, что бинарное отношение $R = \{\langle x, y\rangle \mid x < y$ или $x = y\}$ является частичным порядком на множестве A.

7. Пусть $(A, <)$ — строго частично упорядоченное множество. Элемент $a \in A$ называется *максимальным*, если в A не существует такой элемент b, что $a < b$. Доказать, что если множество A конечно, то в нем существует максимальный элемент.

8. Пусть R — отношение эквивалентности на множестве A. *Классом эквивалентности* элемента $a \in A$ называется множество

$$[a] = \{x \mid \langle a, x\rangle \in R\}.$$

Доказать, что для любых элементов $a, b \in A$ их классы эквивалентности $[a]$ и $[b]$ либо совпадают, либо не имеют общих элементов.

§ 3. Взаимно однозначные соответствия и эквивалентные множества

Функция f называется *взаимно однозначной функцией* (или 1-1-*функцией*), если из $f(x) = f(y)$ следует $x = y$ (выражение $f(x) = f(y)$ означает, что $f(x)$ и $f(y)$ определены и их значения совпадают). Например, id_A является взаимно однозначной функцией. Вообще, функция f взаимно однозначна тогда и только тогда, когда отношение f^{-1} является функцией. Если $f : A \to B$ и $g : B \to C$ суть взаимно однозначные функции, то их композиция $f \circ g$ также есть взаимно однозначная функция.

Взаимно однозначным соответствием между множествами A и B называется такая взаимно однозначная функция $f : A \to B$, что $\rho_f = B$.

Множества A и B называются *равномощными*, если существует взаимно однозначное соответствие между A и B. Чтобы выразить, что A и B равномощны, пишут $A \sim B$.

Теорема 1. *Каковы бы ни были множества A, B, C,*

1) $A \sim A$;

2) *если $A \sim B$, то $B \sim A$;*

3) *если $A \sim B$ и $B \sim C$, то $A \sim C$.*

Доказательство. Легко проверяется справедливость следующих утверждений.

1) Функция id_A является взаимно однозначным соответствием между A и A.

2) Если f — взаимно однозначное соответствие между A и B, то f^{-1} есть взаимно однозначное соответствие между B и A.

3) Если f — взаимно однозначное соответствие между A и B, а g — взаимно однозначное соответствие между B и C, то их композиция $f \circ g$ есть взаимно однозначное соответствие между A и C.

Отсюда немедленно следует утверждение теоремы.

Теорема 1 доказана.

Равномощные множества называются также *эквивалентными*.

§ 4. Счетные множества

Непустое множество называется *счетным*, если оно есть множество значений какой-либо последовательности. Пустое множество по определению относится к счетным.

Пример 1. Любое конечное множество является счетным. Действительно, пусть $M = \{a_0, \ldots, a_{n-1}\}$. Рассмотрим последовательность $f : \mathbb{N} \to M$ такую, что $f(x) = a_l$, где l есть остаток от деления x на n. Очевидно, что $\rho_f = M$.

Пример 2. Натуральный ряд $\mathbb{N}$ — счетное множество, поскольку он является множеством значений функции $id_{\mathbb{N}} : \mathbb{N} \to \mathbb{N}$.

Пример 3. Пусть дан некоторый *алфавит*, т. е. набор элементарных знаков, называемых *буквами*. Конечный ряд букв, написанных друг за другом, называется *словом* в данном алфавите. Иногда бывает удобно рассматривать также пустое слово, совсем не содержащее букв и обычно обозначаемое Λ. Если алфавит A конечен, то множество A^* всех слов в алфавите A счетно.

Действительно, пусть $A = \{S_1, \ldots, S_{p-1}\}$ $(p \geqslant 2)$. Определим последовательность $f : \mathbb{N} \to A^*$ следующим образом: $f(0) = \Lambda$; если же $x > 0$, то рассмотрим запись числа x в p-ичной системе счисления, выпишем в порядке вхождения в нее все ненулевые «цифры» $k_1, \ldots, k_m (1 \leqslant k_i \leqslant p-1)$ и положим $f(x) = S_{k_1} \ldots S_{k_m}$. Очевидно, что $\rho_f = A^*$. А именно, произвольное слово $S_{i_0} \ldots S_{i_n}$ является значением функции f при значении аргумента $i_0 p^n + i_1 p^{n-1} + \cdots + i_n$.

Пример 4. Всякое множество, эквивалентное счетному множеству, счетно. Действительно, пусть A — счетное множество и $A \sim B$. Пусть $f : \mathbb{N} \to A$ — такая последовательность, что $\rho_f = A$, и пусть $g : A \to B$ — взаимно однозначное соответствие между A и B. Нетрудно проверить, что их композиция $f \circ g$ есть последовательность, причем $\rho_{f \circ g} = B$, т. е. B счетно. Отсюда и из примера 2 получаем, в частности, что всякое множество, эквивалентное натуральному ряду, счетно. Например, счетным является множество всех слов в алфавите $\{0, 1, 2, \ldots, 9\}$, являющихся десятичными записями натуральных чисел, поскольку оно, очевидно, эквивалентно натуральному ряду.

Теорема 2. *Любое подмножество счетного множества счетно.*

Доказательство. Пусть A — счетное множество, $B \subseteq A$. Если B — пустое множество, то оно счетно по определению. Рассмотрим случай, когда B непусто. Тогда A также не пусто, и существует последовательность f такая, что $\rho_f = A$. Зафиксируем некоторый элемент $b \in B$ и определим последовательность $g : \mathbb{N} \to B$ следующим образом:

$$g(x) = \begin{cases} f(x), & \text{если } f(x) \in B; \\ l, & \text{если } f(x) \notin B. \end{cases}$$

Очевидно, что $\rho_f = B$, т. е. B счетно. Теорема 2 доказана.

Из теоремы 2 и примера 3 получается еще одно доказательство счетности множества десятичных записей натуральных чисел, поскольку они образуют подмножество множества всех слов в 10-буквенном алфавите $\{0, 1, 2, \ldots, 9\}$.

Пример 5. Множество всех рациональных чисел $\mathbb{Q}$ счетно. Действительно, всякое рациональное число записывается в виде несократимой дроби вида m/n, где m — целое число, а n — положительное целое число, т. е. множество $\mathbb{Q}$ эквивалентно множеству таких дробей, которое, в свою очередь, является подмножеством всех слов в алфавите $\{0, 1, 2, \ldots, 9, -, /\}$. Теперь счетность $\mathbb{Q}$ следует из примера 3, теоремы 2 и примера 4.

Теорема 3. *Объединение счетного числа счетных множеств счетно.*

Доказательство. Пусть дано счетное множество A, элементы которого суть счетные множества. Требуется доказать счетность

множества B, состоящего из всех элементов, принадлежащих элементам множества A. Если A пусто, то B также пусто и счетно по определению. Пусть A непусто и среди его элементов есть непустые множества. Так как A счетно, то существует такая последовательность $h : \mathbb{N} \to A$, что $\rho_h = A$. Обозначим $h(n)$ через A_n $(n \in \mathbb{N})$.

Для любого n, если A_n не пусто, существует такая последовательность $f_n : \mathbb{N} \to A_n$, что $\rho_{fn} = A_n$. Заметим, что B непусто, и зафиксируем некоторый элемент $b \in B$. Если A_n пусто, определим последовательность $f_n : \mathbb{N} \to B$ так, что $f_n(x) = b$ для любого x. Рассмотрим бесконечную таблицу, в строках которой последовательно выписаны значения функций $f_0, f_1, f_2, \ldots$:

x	0		1		2		
$f_0(x)$	$f_0(0)$		$f_0(1)$	$\to$	$f_0(2)$		$\ldots$
	$\downarrow$	$\nearrow$		$\swarrow$		$\nearrow$	
$f_1(x)$	$f_1(0)$		$f_1(1)$		$f_1(2)$		$\ldots$
		$\swarrow$		$\nearrow$		$\swarrow$	
$f_2(x)$	$f_2(0)$		$f_2(1)$		$f_2(2)$		$\ldots$
	$\downarrow$	$\nearrow$		$\swarrow$		$\nearrow$	
$\ldots$	$\ldots$		$\ldots$		$\ldots$		$\ldots$

Очевидно, в этой таблице содержатся все элементы множества B и только они. Пересчитывая элементы таблицы в порядке, указанном стрелками, мы получим последовательность $g : \mathbb{N} \to B$, то есть,

$$g(0) = f_0(0), \quad g(1) = f_1(0), \quad g(2) = f_0(1), \quad g(3) = f_0(2), \quad \ldots .$$

Тем самым доказана счетность множества B. Теорема 3 доказана.

Пример 6. Множество A^* всех слов в счетном алфавите A счетно. Действительно, если A — счетный алфавит, то существует такая последовательность $f : \mathbb{N} \to A$, что $\rho_f = A$. Обозначим $f(n)$ через a_n $(n \in \mathbb{N})$. Пусть $A_n = \{a_0, a_1, \ldots, a_n\}$. Поскольку любое слово в алфавите A состоит лишь из конечного числа букв, оно является одновременно словом в одном из алфавитов A_n. (А именно, слово $a_{k_1} \ldots a_{k_m}$ является словом в конечном алфавите A_k, где $k = \max(k_1, \ldots, k_m)$.) Таким образом, множество всех слов в алфавите A есть объединение счетного числа множеств $A_0^*, A_1^*, A_2^*, \ldots$. Теперь счетность A^* вытекает из примера 3 и теоремы 3.

Теорема 4. *Множество значений функции, определенной на счетном множестве, счетно.*

Доказательство. Пусть A — счетное множество, f – некоторая функция с областью определения A. Поскольку A счетно, существует последовательность $g : \mathbb{N} \to A$ такая, что $\rho_g = A$. Тогда, очевидно, $g \circ f$ есть последовательность, причем $\rho_{g \circ f} = \rho_f$, т. е. множество ρ_f счетно. Теорема доказана.

Пример 7. Действительное число назовем *алгебраическим*, если оно является корнем некоторого многочлена с одним неизвестным и с целыми коэффициентами, т. е. многочлена вида: $a_0x^n + {}$ $+a_1x^{n-1} + \cdots + a_{n-1}x + a_n$ ($a_0, a_1, \ldots, a_n$ — целые числа, $a_0 \neq 0$). Множество алгебраических чисел счетно. Действительно, каждый многочлен можно рассматривать как слово в алфавите $\{0, 1, 2, \ldots$ $\ldots, 9, x, +, -\}$, если вместо x^n писать xn (например, многочлен $4x^5 - 2x^2 + 3$ записывать так: $4x5 - 2x2 + 3$). В силу примера 3 и теоремы 2 множество всех многочленов счетно. Рассмотрим функцию f, определенную на множестве всех многочленов, значением которой на данном многочлене является множество корней этого многочлена (конечное и, следовательно, счетное). По теореме 4 множество ρ_f является счетным. Теперь заметим, что множество всех алгебраических чисел — это в точности объединение всех элементов множества ρ_f, счетное в силу теоремы 3.

Теорема 5. *Все бесконечные счетные множества эквивалентны.*

Доказательство. Докажем, что всякое бесконечное счетное множество эквивалентно натуральному ряду $\mathbb{N}$. Отсюда и из теоремы 1 будет следовать утверждение теоремы.

Пусть A — бесконечное счетное множество, $f : \mathbb{N} \to A$ — такая последовательность, что $\rho_f = A$. Определим новую функцию $g : \mathbb{N} \to A$ следующим образом: $g(0) = f(0)$; $g(n+1) = f(k)$, где k — наименьшее число, такое, что $f(k) \notin \{g(0), \ldots, g(n)\}$ (в силу бесконечности A такое число k существует для любого n). Очевидно, что g — взаимно однозначное соответствие между $\mathbb{N}$ и A. Теорема 5 доказана.

Упражнения.

1. Доказать, что множество всех конечных подмножеств счетного множества счетно.

2. Доказать, что любое множество попарно непересекающихся интервалов на действительной прямой счетно.

3. Доказать, что множество точек разрыва монотонной действительной функции счетно.

§ 5. Канторовский диагональный метод

Теорема 6. *Множество F всех функций из $\mathbb{N}$ в множество $\{0,1\}$ несчетно.*

Доказательство. Предположим, что нам дана некоторая последовательность $f : \mathbb{N} \to F$. Обозначим $f(n)$ через f_n. Подобно тому, как мы поступали при доказательстве теоремы 3, рассмотрим бесконечную таблицу, в строках которой выписаны значения функций $f_0, f_1, f_2, \ldots$. Теперь определим функцию $g \in F$ следующим образом:

$$g(x) = \begin{cases} 1, & \text{если } f_x(x) = 0; \\ 0, & \text{если } f_x(x) = 1. \end{cases}$$

Иными словами, последовательные значения функции g получаются из чисел, стоящих на диагонали таблицы, изменением каждого из них. Функция g не входит в область значений функции f, поскольку $g(p) \neq f_p(p)$, каково бы ни было p. Таким образом, ни для какой последовательности $f : \mathbb{N} \to F$ множество ее значений не совпадает с F, т. е. F несчетно. Теорема 6 доказана.

Метод, использованный в доказательстве теоремы 6, называется *канторовским диагональным методом.*

Следствие. *Множество $\mathcal{P}(\mathbb{N})$ несчетно.*

Доказательство. Достаточно показать, что $\mathcal{P}(\mathbb{N}) \sim F$, а затем воспользоваться примером 4 и теоремой 6. Взаимно однозначное соответствие между $\mathcal{P}(\mathbb{N})$ и F задает функция, сопоставляющая каждому подмножеству $M \subseteq \mathbb{N}$ его характеристическую функцию, т. е. такую функцию $\chi_M \in F$, что

$$\chi_M(x) = \begin{cases} 1, & \text{если } x \in M; \\ 0, & \text{если } x \notin M. \end{cases}$$

§ 6. Кардинальные числа, или мощности

Согласно Кантору, под *кардинальным числом* или *мощностью* множества A понимается то общее, что присуще всем множествам, эквивалентным множеству A. Независимо от способа представления того абстрактного объекта, который называется кардинальным числом, фундаментальное значение имеет то, что два множества A

и B имеют одно и то же кардинальное число, если и только если они эквивалентны, т. е. $A \sim B$.

Кардинальное число (мощность) множества A обозначается через $\bar{\bar{A}}$ или $|A|$. В частности, как мы ранее установили, $|\mathcal{P}(\mathbb{N})| = \bar{\bar{F}}$, где F — множество из теоремы 6.

Если множество A эквивалентно некоторому подмножеству множества B, то пишут $\bar{\bar{A}} \leqslant \bar{\bar{B}}$. Очевидно, что если $A \subseteq B$, то $\bar{\bar{A}} \leqslant \bar{\bar{B}}$. Теорема Кантора–Бернштейна утверждает, что если одновременно $\bar{\bar{A}} \leqslant \bar{\bar{B}}$ и $\bar{\bar{B}} \leqslant \bar{\bar{A}}$, то $\bar{\bar{A}} = \bar{\bar{B}}$. Если A и B не эквивалентны и выполнено неравенство $\bar{\bar{A}} \leqslant \bar{\bar{B}}$, то пишут $\bar{\bar{A}} < \bar{\bar{B}}$.

Согласно теореме 5, все бесконечные счетные множества имеют одну и ту же мощность. Эта мощность обычно обозначается $\aleph_0$ (читается алеф-нуль; $\aleph$ (áлеф) — первая буква еврейского алфавита).

Мощность множества $\mathcal{P}(\mathbb{N})$ (и, следовательно, мощность F) называется *мощностью континуума* и обычно обозначается $\mathfrak{c}$. Можно доказать, что она равна мощности множества всех действительных чисел. Согласно следствию из теоремы 6 $\mathfrak{c} \neq \aleph_0$. Очевидно также, что $\aleph_0 < \mathfrak{c}$.

Предположение о том, что не существует множества M, для которого $\aleph_0 < \bar{\bar{M}} < \mathfrak{c}$, называют *континуум-гипотезой*. Это правдоподобное с интуитивной точки зрения предположение долгое время не удавалось ни доказать, ни опровергнуть. Лишь сравнительно недавно проблема, связанная с континуум-гипотезой, была решена, но в несколько необычном смысле, который разъяснится для нас чуть позже.

Упражнения.

1. Доказать, что если $A_1 \subseteq A_2 \subseteq A$ и $\bar{\bar{A}}_1 = \bar{\bar{A}}$, то $\bar{\bar{A}}_2 = \bar{\bar{A}}$.

2. Доказать теорему Кантора–Бернштейна.

3. Доказать, что объединение счетного числа множеств мощности $\mathfrak{c}$ имеет мощность $\mathfrak{c}$.

§ 7. Теорема Кантора

Теорема 7 (теорема Кантора). *Для любого множества M имеет место $\bar{\bar{M}} < |\mathcal{P}(M)|$.*

Доказательство. Пусть g — такая функция из M в $\mathcal{P}(M)$, что $g(x) = \{x\}$. Эта функция устанавливает взаимно однозначное

соответствие между M и подмножеством $\mathcal{P}(M)$, состоящим из одноэлементных подмножеств M, так что $\bar{\bar{M}} \leqslant |\mathcal{P}(M)|$.

Покажем, что M и $\mathcal{P}(M)$ не эквивалентны. Пусть f — какая-либо функция из M в $\mathcal{P}(M)$, и пусть $S = \{x \mid x \in M$ и $x \notin f(x)\}$. Очевидно, $S \in \mathcal{P}(M)$. Покажем, что $S \notin \rho_f$. Действительно, пусть $f(s) = S$ для некоторого $s \in M$. Простые рассуждения показывают, что в этом случае предположения $s \in S$ и $s \notin S$ оба ведут к противоречию. Таким образом, ни для какой функции $f : M \to \mathcal{P}(M)$ ее множество значений не совпадает с $\mathcal{P}(M)$. Следовательно, не существует взаимно однозначного соответствия между M и $\mathcal{P}(M)$, т. е. они не эквивалентны. Теорема 7 доказана.

Мощность множества $\mathcal{P}(M)$ принято обозначать $2^{\bar{\bar{M}}}$. Таким образом, $\bar{\bar{M}} < 2^{\bar{\bar{M}}}$. В частности, $\aleph_0 < 2^{\aleph_0} < 2^{2^{\aleph_0}} < \ldots$. Заметим, что кардинальное число $2^{\aleph_0}$ равно мощности континуума.

§ 8. Парадоксы теории множеств

В 90-х годах XIX в., когда теория множеств стала получать признание среди математиков, в ней были обнаружены противоречия. Рассмотрим некоторые из них.

Парадокс Кантора связан с множеством всех множеств. Обозначим это множество через T. Тогда $\mathcal{P}(T)$ есть некоторое множество множеств, откуда $\mathcal{P}(T) \subseteq T$. Но тогда $|\mathcal{P}(T)| \leqslant \bar{\bar{T}}$. С другой стороны, для любого множества M имеет место неравенство $\bar{\bar{M}} \leqslant |\mathcal{P}(M)|$. Отсюда по теореме Кантора–Бернштейна получается $\bar{\bar{T}} = |\mathcal{P}(T)|$, что противоречит теореме 7.

Вот еще один парадокс теории множеств — *парадокс Рассела.* Пусть R есть множество всех множеств, которые не являются элементами самих себя, т. е. $R = \{x | x \notin x\}$. Тогда оказывается, что $R \in R$ выполняется тогда и только тогда, когда $R \notin R$.

Парадоксы Кантора, Рассела и другие теоретико-множественные парадоксы демонстрируют трудности, связанные с попытками построить теорию множеств на основе интуитивного понятия множества. Эти трудности вынуждают нас заняться вопросом: в чем же собственно подвели нас методы образования понятий и рассуждения, казавшиеся убедительными, пока не выяснилось, что они приводят к парадоксам? Различные математики высказывали разные взгляды по поводу причин возникновения парадоксов и предлагали некоторые способы избавления от них.

Один из возможных путей избавления от известных парадоксов состоит в различении совокупностей двух сортов, называемых классами и множествами. Точнее, произвольная совокупность объектов считается *классом*, а множествами являются только те из классов, которые сами могут быть элементами других классов. При таком подходе рассуждения, используемые в парадоксах Кантора и Рассела, приводят не к противоречию, а всего лишь к результату о том, что некоторые совокупности не являются множествами. Чтобы убедиться, что это не просто игра терминами, попытаемся, например, провести парадокс Рассела, имея в виду, что совокупность R всех множеств, не являющихся элементами самих себя, — не множество, а, как говорят, собственный класс — класс, не являющийся множеством. Очевидно, что R не является своим элементом, потому что никакой собственный класс не может быть элементом никакого класса. Отсюда, однако, не следует, что мы должны включить его в R в качестве элемента, потому что к классу R мы относим только множества. Так что никакого противоречия здесь нет.

§ 9. Аксиоматическая теория множеств

Поскольку свободное пользование понятиями, исходящими из интуитивных представлений о множествах, приводит к противоречиям, Э. Цермело (1908 г.) предложил ограничиться рассмотрением множеств, существование которых может быть доказано на основе некоторого списка аксиом. Предложенная Цермело система аксиом впоследствии была несколько расширена А. Френкелем и носит название системы Цермело–Френкеля *ZF*. Основными (неопределяемыми) понятиями этой системы являются отношение принадлежности $\in$ и отношение равенства $=$. Система *ZF* имеет следующие аксиомы.

I. *Аксиома объемности.* Два множества равны, если и только если они состоят из одних и тех же элементов.

II. *Аксиома пары.* Для любых множеств A и B существует такое множество, что A и B являются единственными его элементами.

III. *Аксиома объединения.* Для любого множества A существует множество $\cup A$, состоящее в точности из всех элементов, принадлежащих элементам множества A.

IV. *Аксиома множества всех подмножеств.* Для любого множества A существует множество $\mathcal{P}(A)$ всех подмножеств A.

V. *Аксиома выделения.* Для любого множества A и свойства Φ такого, что для любого $x \in A$ утверждение $\Phi(x)$ либо истино, либо ложно, существует множество $\{x \mid x \in A \text{ и } \Phi(x)\}$, состоящее в точности из тех элементов A, для которых Φ истинно.

VI. *Аксиома бесконечности.* Существует по крайней мере одно бесконечное множество — множество натуральных чисел $\{0, 1, 2, ...\}$.

VII. *Аксиома выбора.* Для любого непустого множества S попарно непересекающихся множеств существует некоторое множество, содержащее в качестве своих элементов ровно по одному элементу из каждого элемента множества S.

VIII. *Аксиома фундирования.* Не существует бесконечной убывающей последовательности $x_1 \ni x_2 \ni \ldots$.

IX. *Аксиома подстановки.* Для каждого множества A и функции f, определенной на A, существует множество, содержащее в точности объекты $f(x)$ для $x \in A$.

Все аксиомы могут быть записаны совершенно формально — а именно, формулами языка теории множеств, описанного в § 7 следующей главы. Эта и другие известные системы аксиом для теории множеств сформулированы так, чтобы на их основе можно было доказать все обычные теоремы теории множеств, но без парадоксов.

Хотя в теории множеств, основанной на аксиомах I–IX, никаких противоречий не обнаружено, это еще не означает, что противоречия здесь невозможны. Чтобы установить недоказуемость противоречия, нужно прежде всего уточнить понятие доказательства, т. е. правильного рассуждения. Ведь пока мы не уточним, что такое «доказательство», мы не сможем строго математически доказать, что нечто невозможно доказать. Значит, необходимо строгое определение доказательства, нужна наука о доказательствах, о правильных рассуждениях, т. е. логика.

В заключение вернемся к вопросу, связанному с континуум-гипотезой. Именно с помощью уточнения понятия доказательства и методов математической логики в работах К. Гёделя и П. Коэна было доказано, что континуум-гипотеза не может быть ни доказана, ни опровергнута на основе обычных аксиом теории множеств. Это не единственный пример того, как математическая логика помогла получить нетрадиционное решение известных математических проблем.

Упражнение. На основе системы аксиом ZF доказать, что каковы бы ни были множества A, B, C, если $A \in B$ и $B \in C$, то $C \notin A$.

ГЛАВА 2

ЯЗЫКИ ПЕРВОГО ПОРЯДКА

§ 1. Высказывания и высказывательные формы

Чтобы логику можно было развивать математическими методами, необходимо прежде всего уточнить основные логические понятия. Нашей основной задачей является уточнение и изучение понятия правильного рассуждения, или доказательства. Всякое рассуждение состоит в последовательном переходе от одной мысли к другой, или, как говорят в логике, от одного суждения к другому. Материальным выражением суждения является предложение того или иного языка. Например, математические суждения мы обычно записываем в виде текстов на русском языке, обогащенном математической символикой. Предложения, выражающие определенные суждения, называются *высказываниями.* Они характеризуются тем, что могут быть истинными или ложными, и этим отличаются, например, от повелительных или вопросительных предложений.

Например, $2 \times 2 = 4$, «Рим — столица Франции» суть высказывания, а предложения «Который час?» или «Решить квадратное уравнение $x^2 + 3x - 2 = 0$» высказываниями не являются.

Если высказывание истинно, говорят, что его *истинностное значение* есть И («истина»), а если высказывание ложно, то его истинностное значение есть Л («ложь»). Например, высказывание $2 \times 2 = 4$ имеет истинностное значение И, а высказывание «Рим — столица Франции» — Л.

Однако, не всякое повествовательное предложение является высказыванием. Рассмотрим, например, предложение: «Остаток от деления числа n на 7 равен 3». В этом предложении не содержится никакого утверждения, и нельзя ставить вопрос о его истинности и ложности. Однако, подставив в это предложение вместо n обозначение какого-либо конкретного натурального числа, мы получим высказывание.

Буква n, входящая в это предложение, играет роль переменной. Вообще, *переменная* — это языковое выражение, служащее для обозначения произвольного объекта из некоторого фиксированного множества, называемого областью возможных значений этой пере-

менной. Если переменная употребляется таким образом, что допускается подстановка вместо нее обозначений (*имен*) объектов из области ее возможных значений, то эта переменная называется *свободной.* Таковы, например, переменные x, y, z в выражениях $x < y$ и $z = x + 1$. Однако в математике встречается и такое употребление переменных, при котором не предполагается и не допускается возможность подстановки вместо них имен конкретных объектов. Например, в выражение $\int\limits_0^3 x^2\,dx$, где x — действительная переменная, т. е. переменная, областью возможных значений которой является множество действительных чисел, нельзя подставлять вместо x обозначения каких-либо конкретных действительных чисел. Вот другой пример: «Не существует такого рационального числа q, что $q^2 = 2$». Хотя это предложение и содержит переменную q, подстановка в него обозначений каких-либо чисел вместо q лишена смысла. В том случае, когда по смыслу выражения, содержащего переменную, подстановка вместо нее имен конкретных объектов недопустима, эта переменная называется *связанной.* В одном выражении одна и та же переменная может употребляться и как свободная, и как связанная. Например, в выражении $\int\limits_0^x x^2\,dx$ оба вхождения переменной x в подынтегральное выражение являются связанными, а ее вхождение в качестве верхнего предела интегрирования — свободным. Вообще, следует говорить именно о свободных и связанных *вхождениях* данной переменной в данное выражение.

Выражение, содержащее свободные вхождения переменных и превращающееся в имя некоторого объекта (или, соответственно, высказывание) всякий раз, когда вместо всех свободных вхождений каждой переменной подставляется имя какого-нибудь объекта из области ее возможных значений, называется *именной формой* (или, соответственно, *высказывательной формой*). Переменные, имеющие свободные вхождения в именную или высказывательную форму, называются ее *параметрами.* Именную или высказывательную форму будем называть *k-местной*, если она содержит ровно k различных параметров. В частности, можно говорить и о 0-местных именных и высказывательных формах, понимая под ними соответственно имена и высказывания.

Иногда для k-местной именной или высказывательной формы мы будем употреблять обозначение вида $F(x_1, \ldots, x_k)$, явно указывая все ее параметры. Тогда, если $a_1, \ldots, a_k$ — имена каких-либо объектов из областей возможных значений переменных $x_1, \ldots, x_k$ со-

ответственно, то через $F(a_1, \dots, a_k)$ обозначается выражение, полученное из $F(x_1, \dots, x_k)$ подстановкой a_1 вместо $x_1, \dots, a_k$ вместо x_k.

Пример 1. Через $F(x, y)$ обозначим именную форму

$$y + x \cdot y \cdot \lim_{y \to 5} \int_x^y \sin x^2 y \, dx.$$

Тогда $F(-7, 3)$ есть выражение

$$3 + (-7) \cdot 3 \cdot \lim_{y \to 5} \int_{-7}^y \sin x^2 y \, dx.$$

Вообще, $F(a, b)$ имеет вид

$$b + a \cdot b \cdot \lim_{y \to 5} \int_a^y \sin x^2 y \, dx.$$

Пример 2. Через $A(i, k, m)$ обозначим высказывательную форму

$$\sum_{i=k}^{m} \frac{1}{i^2} < \lim_{k \to i} \log_2 k.$$

Тогда, например, $A(5, 2, 8)$ есть высказывание

$$\sum_{i=2}^{8} \frac{1}{i^2} < \lim_{k \to 5} \log_2 k.$$

§ 2. Логические операции

Из одних высказываний различными способами можно строить новые более сложные высказывания. Способ построения сложного высказывания из данных высказываний, при котором истинностное значение сложного высказывания полностью определяется истинностными значениями исходных высказываний, называется *логической операцией*.

Примером логической операции может служить *отрицание*, преобразующее любое данное высказывание A в высказывание «Неверно, что A», которое мы будем обозначать $\neg A$. Очевидно, что

высказывание $\neg A$ истинно тогда и только тогда, когда A ложно. Этот факт можно выразить посредством следующей *истинностной таблицы*:

A	$\neg A$
И	Л
Л	И

Эта таблица показывает, какое истинностное значение имеет высказывание $\neg A$ при данном истинностном значении высказывания A.

Вообще, для любой логической операции можно построить соответствующую ей истинностную таблицу. Некоторые из наиболее употребительных логических операций имеют специальные названия и обозначения. Кроме отрицания, это еще двуместные операции: *коньюнкция* $(\&, \wedge)$, *дизъюнкция* $(\vee)$, *импликация* $(\supset, \rightarrow, \Rightarrow)$, *эквивалентность* $(\equiv, \leftrightarrow, \Leftrightarrow)$. Им соответствуют следующие истинностные таблицы:

A	B	$A \,\&\, B$	$A \vee B$	$A \supset B$	$A \equiv B$
И	И	И	И	И	И
И	Л	Л	И	Л	Л
Л	И	Л	И	И	Л
Л	Л	Л	Л	И	И

В математической логике принято не различать логические операции с одинаковыми истинностными таблицами независимо от того, какое словесное оформление имеют эти логические операции. Например, высказывание $A \supset B$ может передаваться посредством выражений «Если A, то B», «A влечет B», «В случае A имеет место B», «Для A необходимо B», «A, только если B» и т. п. Вот языковые эквиваленты для других логических операций: $\neg A$ — «Не A», «A не имеет места», «A неверно»; $A \,\&\, B$ — «A и B», «Не только A, но и B», «Как A, так и B»; $A \vee B$ — «A или B или оба», «A или B», «A, если не B»; $A \equiv B$ — «A, если и только если B», «Если A, то и B, и обратно», «A эквивалентно B», «A равносильно B», «A тогда и только тогда, когда B».

Наконец, приведем пример операции над высказываниями, которая не является логической операцией: по высказыванию A строим высказывание «Я знаю, что A». Очевидно, что истинность или ложность такого высказывания зависит не только от истинностного значения A, но и от осведомленности субъекта, произносящего это высказывание.

Рассмотренные нами логические операции $\neg, \&, \vee, \supset, \equiv$ называются *пропозициональными операциями*, а символы используемые

для их обозначения, — *пропозицональными связками.* Эти операции можно, очевидно, применять и к высказывательным формам, получая из них более сложные высказывательные формы.

Упражнение. Найти истинностные значения следующих высказываний:

а) Если 11 делится на 3, то 11 делится на 6.

б) Если 15 делится на 3, то 15 делится на 6.

в) 11 делится на 3 тогда и только тогда, когда 15 делится на 6.

§ 3. Логика высказываний

Переменная, допустимыми значениями которой являются произвольные высказывания, называется *пропозициональной переменной.* В качестве пропозициональных переменных мы будем использовать большие латинские буквы $P, Q, R, \ldots$ (возможно с индексами; например, P_3, Q_7, R_{11}).

Формулами логики высказываний, или *пропозициональными формулами*, назовем выражения, которые строятся из пропозициональных переменных с помощью скобок и пропозициональных связок по следующим правилам:

1) любая пропозициональная переменная является пропозициональной формулой;

2) если $\mathcal{A}$ и $\mathcal{B}$ — пропозициональные формулы, то $\neg\mathcal{A}$, $(\mathcal{A} \mathbin{\&} \mathcal{B})$, $(\mathcal{A} \vee \mathcal{B})$, $(\mathcal{A} \supset \mathcal{B})$, $(\mathcal{A} \equiv \mathcal{B})$ — пропозициональные формулы.

Например, выражения

$$(P \supset Q), \quad (P \supset (Q \supset R)), \quad (P \supset (Q \supset (P \mathbin{\&} Q)))$$

являются пропозициональными формулами.

Если в пропозициональную формулу $\mathcal{A}$, построенную из пропозициональных переменных $P_1, \ldots, P_n$, вместо этих переменных подставить конкретные высказывания, то получится некоторое высказывание. Пропозициональная формула называется *тавтологией*, если она превращается в истинное высказывание при любой подстановке конкретных высказываний вместо переменных; каждая тавтология является схемой истинных высказываний и в этом смысле выражает некоторый *логический закон.* Приведем примеры логических законов: $(P \vee \neg P)$ — закон исключенного третьего; $(\neg\neg P \equiv P)$ — закон двойного отрицания; $\neg(P \mathbin{\&} \neg P)$ — закон противоречия; $(((P \supset Q) \supset P) \supset P)$ — закон Пирса.

Очевидно, что истинностное значение высказывания, полученного подстановкой в пропозициональную формулу конкретных высказываний вместо пропозициональных переменных, зависит только от истинностных значений подставляемых высказываний. Поэтому довольно легко можно проверить, является ли данная пропозициональная формула тавтологией. Для этого достаточно перебрать всевозможные подстановки в эту формулу значений И и Л вместо пропозициональных переменных (таких подстановок ровно 2^n, где n — число переменных в формуле), и для каждой такой подстановки вычислить соответствующее значение формулы, пользуясь истинностными таблицами для логических операций. Формула является тавтологией тогда и только тогда, когда при любой подстановке она принимает значение И.

Упражнения.

1. Доказать *интерполяционную теорему*: если пропозициональная формула $\mathcal{A} \supset \mathcal{B}$ — тавтология, и формулы $\neg\mathcal{A}$ и $\mathcal{B}$ не являются тавтологиями, то существует пропозициональная формула $\mathcal{C}$, содержащая только те переменные, которые входят как в $\mathcal{A}$, так и в $\mathcal{B}$, такая, что формулы $\mathcal{A} \supset \mathcal{C}$ и $\mathcal{C} \supset \mathcal{B}$ суть тавтологии.

2. Множество пропозициональных формул называется *совместным*, если существуют такие истинностные значения пропозициональных переменных, при которых все формулы из этого множества принимают значение И. Доказать *теорему компактности*: множество пропозициональных формул совместно тогда и только тогда, когда каждое его конечное подмножество совместно.

§ 4. Кванторы

Наряду с пропозициональными операциями в математической логике рассматриваются *кванторы*, позволяющие из данной высказывательной формы получать высказывательную форму с меньшим числом параметров, в частности, из одноместной высказывательной формы — высказывание.

Квантор общности позволяет из данной высказывательной формы с единственным параметром x получить высказывание с помощью оборота «Для всех $x\ldots$». Результат применения квантора общности к высказывательной форме $A(x)$ будем обозначать $\forall x\ A(x)$. Высказывание $\forall x\ A(x)$ считается истинным тогда и только тогда,

когда при подстановке в $A(x)$ вместо свободных вхождений переменной x имени любого объекта из области ее возможных значений всегда получается истинное высказывание. Высказывание $\forall x\ A(x)$ может читаться также «Для любого x имеет место $A(x)$», «$A(x)$ при произвольном x», «Для всех x верно $A(x)$», «Каждый x обладает свойством $A(x)$» и т. п.

Квантор существования соответствует образованию из данной высказывательной формы с единственным параметром x высказывания с помощью оборота «Существует такой x, что … ». Результат применения квантора существования к высказывательной форме $A(x)$ обозначается $\exists x\ A(x)$. Высказывание $\exists x\ A(x)$ истинно тогда и только тогда, когда в области возможных значений переменной x найдется такой объект, что при подстановке его имени вместо свободных вхождений x в $A(x)$ получается истинное высказывание. Высказывание $\exists x\ A(x)$ может читаться также «Для некоторых x имеет место $A(x)$», «Для подходящего x верно $A(x)$», «Существует x, для которого $A(x)$», «Хотя бы для одного x верно $A(x)$» и т. п.

Отметим еще раз, что в предложениях $\forall x\ A(x)$ и $\exists x\ A(x)$ переменная x не является свободной переменной: кванторы «связывают» эту переменную. Очевидно также, что кванторы можно применять и к высказывательным формам, содержащим наряду с x и другие параметры. В результате получится высказывательная форма, имеющая те же параметры, что и исходная, кроме x.

Важное значение для логики имеет анализ логической структуры высказываний и высказывательных форм, т. е. выявление того, каким образом данное повествовательное предложение построено из более простых предложений с помощью пропозициональных операций и кванторов. Логический анализ предложений есть своего рода искусство, практические навыки которого можно приобрести путем упражнений. Рассмотрим некоторые примеры. Высказывание «2 — простое число, а 6 — составное число», очевидно, может быть представлено в виде «2 — простое число» & «6 — составное число». Предложение «Каждое рациональное число есть действительное число» можно иначе записать так:

$$\forall x\ \big[(x \text{ — рациональное число}) \supset (x \text{ — действительное число})\big],$$

а предложение «Некоторые действительные числа яваляются рациональными» — так:

$$\exists x\ \big[(x \text{ — действительное число}) \,\&\, (x \text{ — рациональное число})\big].$$

Упражнение. Найти истинностные значения следующих высказываний, где возможными значениями переменных являются действительные числа:

а) $\forall x\ \exists y\ (x + y = 3)$;
б) $\exists y\ \forall x\ (x + y = 7)$;
в) $\exists x\ \exists y\ (x + y = 11)$;
г) $\forall x\ \forall y\ (x + y = 3) \supset 7 = 11$;
д) $\forall a\ (\exists x\ (ax = 3) \equiv a \neq 0)$;
е) $\exists a\ \forall b\ \exists x\ (x^2 + ax + b = 0)$.

§ 5. Субъектно-предикатная структура предложений

Логический анализ предложений во многом аналогичен грамматическому анализу сложно-сочиненных и сложно-подчиненных предложений. Однако иногда нас будет интересовать и внутренняя структура простых предложений: *что* и *о чем* говорится в данном предложении. В таком случае в грамматике используются понятия субъекта и предиката. *Субъект* (или подлежащее) — это то, о чем или о ком говорится в предложении, а *предикат* (называемый также сказуемым или группой сказуемого) выражает то, что говорится о субъекте. В математической логике используется более широкая трактовка субъектно-предикатной структуры предложения. Прежде всего, в качестве субъектов данного предложения мы можем выделить одно или несколько имен каких-либо предметов, входящих в это предложение. Заменив затем выделенные имена на переменные, мы получим высказывательную форму, «в чистом виде» выражащую то, что говорится о субъекте. Эту высказывательную форму тоже иногда называют предикатом.

Рассмотрим, например, высказывание «12 делится на 3», которое, используя общепринятую символику, можно записать так: «$12 \vdots 3$». Выбрав в качестве субъекта число 12, мы получаем одноместный предикат «$x \vdots 3$». Если же в качестве субъекта взять 3, то получим другой предикат «$12 \vdots y$». Наконец, считая 12 и 3 субъектами этого предложения, мы получаем двуместный предикат «$x \vdots y$».

Со всяким предикатом, понимаемым как высказывательная форма, естественным образом связана функция, которая каждому набору значений параметров сопоставляет высказывание, получающееся из данной высказывательной формы подстановкой вместо переменных имен объектов, выбранных в качестве значений этих параметров. Обобщая это наблюдение, мы приходим к представлению о предикате как о функции, значениями которой являются высказывания. Наконец, если мы не будем различать высказывания, имеющие одно и то же истинностное значение, то придем к следующему

определению предиката: k-местным *предикатом* на множестве M называется произвольная функция $P : M^k \to \{\text{И}, \text{Л}\}$, где M^k — декартова степень множества M, т. е. прямое произведение k одинаковых множеств, равных M.

Пример 1. На произвольном множестве M может быть определен двуместный предикат $E : M^2 \to \{\text{И}, \text{Л}\}$ так, что $E(x, y) = \text{И}$ тогда и только тогда, когда x и y совпадают. Этот предикат называют предикатом равенства и обычно вместо $E(x, y)$ пишут $x = y$.

Пример 2. На произвольной совокупности множеств M можно определить двуместный предикат $P : M^2 \to \{\text{И}, \text{Л}\}$ так, что $P(x, y) = \text{И}$ тогда и только тогда, когда x является элементом y. Этот предикат называют предикатом принадлежности и вместо $P(x, y)$ пишут $x \in y$.

Пример 3. В соответствии с нашим определением предиката рассмотренный выше предикат $x \vdots y$ можно трактовать как функцию $D : \mathbb{N}^2 \to \{\text{И}, \text{Л}\}$ такую, что $D(x, y) = \text{И}$ тогда и только тогда, когда x делится на y. Например, $D(12, 3) = \text{И}$, а $D(7, 3) = \text{Л}$.

Вообще, всякий раз, когда речь идет о «свойствах» объектов или «отношениях» между ними, их можно представлять как соответствующие предикаты. Например, свойство «быть четным числом» можно представить как такой предикат $\text{Ч} : \mathbb{N} \to \{\text{И}, \text{Л}\}$, что

$$\text{Ч}(x) = \begin{cases} \text{И}, & \text{если } x \text{ четно;} \\ \text{Л}, & \text{если } x \text{ нечетно.} \end{cases}$$

§ 6. Языки первого порядка

Рассмотренные нами логические понятия, подходящим образом уточненные, служат основой для превращения логики в математическую науку. Прежде всего сделаем точными математическими объектами математические утверждения. С этой целью в математической логике используются искусственные языки. Самый распространенный вид таких языков — так называемое *логико-математические языки первого порядка.*

Каждый язык первого порядка задается своей *сигнатурой* — набором из трех множеств $\Omega = \langle \text{Cnst}, \text{Fn}, \text{Pr} \rangle$, где

1) Cnst — множество *констант*;

2) Fn — множество *функциональных символов*;

3) Pr — множество *предикатных символов.*

При этом с каждым функциональным или предикатным символом однозначно связано некоторое натуральное число — количество аргументов (или *валентность*, арность) этого символа. Валентность функционального символа положительна, а предикатные символы могут иметь и нулевую валентность. Функциональный или предикатный символ, валентность которого равна k, называют k-местным.

Во всяком языке первого порядка имеется счетный набор *переменных.* Условимся считать, что в качестве переменных во всех языках первого порядка используются строчные буквы из конца латинского алфавита с числовыми индексами или без них.

Язык первого порядка с сигнатурой Ω будем называть языком Ω.

Из переменных, констант, функциональных и предикатных символов с помощью скобок (,), запятых и *логических символов* $=$, $\neg$, $\&$, $\vee$, $\supset$, $\equiv$, $\forall$, $\exists$ строятся выражения, называемые термами и формулами. При этом термы играют роль имен и именных форм, а формулы — роль высказываний и высказывательных форм.

Определение *терма* носит индуктивный характер и содержит три пункта. Первые два пункта являются базисом индукции и указывают, какие объекты языка следует непосредственно считать термами. Третий пункт представляет собой шаг индукции и задает *порождающее правило*, позволяющее из уже построенных термов построить новый терм:

1. Каждая переменная есть терм.

2. Каждая константа есть терм.

3. Если f есть k-местный функциональный символ и $t_1, \ldots, t_k$ — термы, то выражение $f(t_1, \ldots, t_k)$ есть терм.

Пример. Пусть сигнатура содержит константу c и двуместные функциональные символы g и h, и пусть x, y — переменные. Тогда выражения

$$c,\ x,\ y,\ h(c,x),\ h(c,c),\ h(c,y),\ g(x,h(c,y)),\ g(h(c,x),g(x,y))$$

суть термы.

Индуктивный характер определения терма дает возможность использовать в доказательствах *принцип индукции по построению.* А именно, пусть требуется доказать, что все термы обладают некоторым свойством P. Для этого достаточно установить, что

1) каждая переменная обладает свойством P;

2) каждая константа обладает свойством P;

3) если $t_1, \ldots, t_n$ — термы, обладающие свойством P, а f есть n-местный функциональный символ, то терм $f(t_1, \ldots, t_n)$ также обладает свойством P.

Тогда в силу индуктивного определения терма можно быть уверенным, что всякий терм обладает свойством P.

Аналогично индуктивный характер определения терма позволяет индукцией по построению терма задавать функции, определенные на множестве всех термов. А именно, пусть

1) каждой переменной x поставлен в соответствие некоторый объект F_x;

2) каждой константе c поставлен в соответствие некоторый объект F_c;

3) задано правило, определяющее, какой объект $F_{f(t_1,\ldots,t_n)}$ ставится в соответствие терму $f(t_1, \ldots, t_n)$, если термам $t_1, \ldots, t_n$ уже поставлены в соответствие объекты $F_{t_1}, \ldots, F_{t_n}$. Тогда для любого терма t однозначно определен объект F_t.

Атомные (или *элементарные*) *формулы* определяются как выражения вида $P(t_1, \ldots, t_k)$, где P есть k-местный предикатный символ ($k \geqslant 1$), а $t_1, \ldots, t_k$ — термы. Всякий 0-местный предикатный символ также считается атомной формулой. Кроме того, к числу атомных формул относятся выражения вида $t_1 = t_2$, где t_1 и t_2 — термы.

Формулы определяются индуктивно с помощью следующих четырех пунктов, причем первый пункт представляет собой базис индукции, а остальные три пункта суть порождающие правила.

1. Каждая атомная формула есть формула.
2. Если $\mathcal{A}$ — формула, то выражение $\neg\mathcal{A}$ есть формула.
3. Если $\mathcal{A}$ и $\mathcal{B}$ — формулы, то выражения $(\mathcal{A} \,\&\, \mathcal{B})$, $(\mathcal{A} \vee \mathcal{B})$, $(\mathcal{A} \supset \mathcal{B})$, $(\mathcal{A} \equiv \mathcal{B})$ суть формулы.
4. Если $\mathcal{A}$ — формула, x — переменная, то выражения $\forall x\ \mathcal{A}$ и $\exists x\ \mathcal{A}$ суть формулы.

Пример. Если сигнатура содержит двуместный функциональный символ f, одноместный предикатный символ P и двуместный предикатный символ Q, то следующие выражения являются формулами:

$$P(f(x,y)), \quad Q(x,z), \quad x = y, \quad \exists y\ x = y,$$
$$\exists x\ Q(x,z), \quad (P(f(x,y)) \,\&\, \exists x\ Q(x,z)),$$
$$((P(f(x,y)) \,\&\, \exists x\ Q(x,z)) \supset \exists y\ x = y),$$
$$\exists z\ ((P(f(x,y)) \,\&\, \exists x\ Q(x,z)) \supset \exists y\ x = y).$$

Индуктивный характер определения формулы позволяет использовать в рассуждениях индукцию по построению формулы. А именно, если требуется доказать, что все формулы обладают некоторым свойством P, то достаточно установить, что

1) каждая атомная формула обладает свойством P;

2) если формула $\mathcal{A}$ обладает свойством P, то формула $\neg\mathcal{A}$ также обладает свойством P;

3) если формулы $\mathcal{A}$ и $\mathcal{B}$ обладают свойством P, то формулы $(\mathcal{A} \mathbin{\&} \mathcal{B})$, $(\mathcal{A} \vee \mathcal{B})$, $(\mathcal{A} \supset \mathcal{B})$, $(\mathcal{A} \equiv \mathcal{B})$ также обладают свойством P;

4) если формула $\mathcal{A}$ обладает свойством P, а x — произвольная переменная, то формулы $\forall x\ \mathcal{A}$ и $\exists x\ \mathcal{A}$ обладают свойством P.

Индукцией по построению формулы можно также задавать функции, определенные на множестве всех формул.

Практически, записывая формулы, принято опускать некоторые скобки. Полученные при этом выражения следует рассматривать как сокращенное обозначение для формул. В частности, обычно опускают внешние скобки у формул. Дальнейшая «экономия» скобок возможна, если принять соглашение о том, какие логические операции «сильнее». Для этого расположим логические символы в следующем порядке:

$$\forall\ \exists\ \neg\ \&\ \vee\ \supset\ \equiv$$

и будем считать, что из всех возможных «в первую очередь» выполняется та операция, которая стоит в этом списке левее. (На самом деле кванторы $\forall$, $\exists$ и отрицание $\neg$ никогда не могут «конкурировать» друг с другом.)

Пример. Формулу

$$(\forall x\ (x = y \supset (\exists z\ Q(z) \mathbin{\&} (R(x) \equiv Q(y)))) \vee Q(x))$$

можно сокращенно изобразить в виде

$$\forall x\ (x = y \supset \exists z\ Q(z) \mathbin{\&} (R(x) \equiv Q(y))) \vee Q(x).$$

В формулах вида $\forall x\ \mathcal{A}$ и $\exists x\ \mathcal{A}$ выражение $\forall x$ или $\exists x$ называется *кванторной приставкой*, а формула $\mathcal{A}$ — *областью действия* соответствующего квантора (точнее — кванторной приставки).

Вхождение переменной x в формулу $\mathcal{A}$ называется *связанным*, если оно находится в области действия квантора $\forall x$ или $\exists x$ или входит в кванторную приставку. Вхождение переменной, не являющееся связанным, называется *свободным*.

Пример. В формуле

$$\forall \underline{\underline{x}}\ (P(f(\underline{\underline{x}}))\ \&\ \exists \underline{x}\ \underline{x} = z \supset \exists \underline{\underline{x}}\ R(\underline{\underline{x}}, \underline{\underline{x}})) \vee z = x$$

подчеркнуты все связанные вхождения переменной x, причем вхождения, связанные одной и той же кванторной приставкой, подчеркнуты одинаковым числом черточек. Неподчеркнутое вхождение x, а также все вхождения z являются свободными.

Формула, не содержащая свободных переменных, называется *замкнутой* (или *закрытой*) *формулой.*

Выражение вида $\binom{x_1 \ \dots \ x_n}{t_1 \ \dots \ t_n}$, где $x_1, \dots, x_n$ — различные переменные, $t_1, \dots, t_n$ — термы, назовем *подстановкой.*

Пусть E — терм (формула) языка Ω, $\theta = \binom{x_1 \ \dots \ x_n}{t_1 \ \dots \ t_n}$ — подстановка. Через θE обозначим выражение, полученное одновременной заменой в E всех (свободных) вхождений переменных $x_1, \dots, x_n$ на термы $t_1, \dots, t_n$ соответственно. Очевидно, что если $t_1, \dots, t_n$ — термы языка Ω, а E — формула языка Ω, то θE — также формула языка Ω, а если E — терм языка Ω, то θE также является термом языка Ω. Выражение θE называется *результатом подстановки* термов $t_1, \dots, t_n$ вместо переменных $x_1, \dots, x_n$ в E. Заметим, что терм (формула) θE зависит лишь от того, какие термы подставляются вместо переменных, имеющих (свободные) вхождения в терм (формулу) E. В частности, если $\mathcal{A}$ — замкнутая формула, то $\theta\mathcal{A}$ совпадает с $\mathcal{A}$, какова бы ни была подстановка θ.

Примеры.

1. Пусть E есть формула $\exists y\ P(x, y, z)$, а $\theta = \binom{x}{f(x,y)}$. Тогда θE есть формула $\exists y\ P(f(x, y), y, z)$.

2. Если E есть $x = y \supset \forall y\ Q(y)$, а $\theta = \binom{x \quad y}{f(x,y) \quad z}$, то θE — это формула $f(x, y) = z \supset \forall y\ Q(y)$.

3. Если E — это формула $\forall y\ P(y, z) \vee \exists y\ R(x, y)$, а θ — подстановка из примера 2, то θE — это формула

$$\forall y\ P(y, z) \vee \exists y\ R(f(x, y), y).$$

Терм t называется *свободным для переменной* x *в формуле* $\mathcal{A}$, если никакое свободное вхождение x в $\mathcal{A}$ не находится в области действия кванторов по переменным, входящим в терм t. Например, терм $f(x, z)$ является свободным для x в формуле $\exists y\ P(x, y, z)$ и не является свободным для x в формуле $\exists z\ P(x, y, z)$. В дальнейшем мы увидим, что с логической точки зрения подстановка терма t

вместо x в формулу $\mathcal{A}$ является правильной и осмысленной, только если t свободен для x в $\mathcal{A}$.

Иногда, имея в виду дальнейшее применение подстановки

$$\theta = \begin{pmatrix} x_1 & \ldots & x_n \\ t_1 & \ldots & t_n \end{pmatrix}$$

к некоторому терму или формуле E, для E употребляют обозначение $E(x_1, \ldots, x_n)$ и затем вместо θE пишут $E(t_1, \ldots, t_n)$.

Упражнения.

1. Какие вхождения переменных являются свободными, а какие связанными в следующих формулах:

а) $\forall x\ (P(x,y) \supset \forall y\ Q(y))$;

б) $\forall x\ P(x,y) \supset \forall y\ R(x,y)$;

в) $\neg\exists z\ Q(z,z) \mathbin{\&} R(f(y,z))$?

2. Является ли терм t свободным для переменной y в $\mathcal{A}$, если

а) t есть $f(x,y)$, $\mathcal{A}$ есть $\forall x\ P(x,y)$;

б) t есть $f(y,z)$, $\mathcal{A}$ есть $P(y,z) \supset \exists z\ Q(z)$?

3. Доказать, что

а) терм, не содержащий переменных, свободен для любой переменной в любой формуле;

б) x свободна для x в любой формуле;

в) если формула $\mathcal{A}$ не содержит свободных вхождений x, то любой терм свободен для x в $\mathcal{A}$.

4. Назовем подстановку $\binom{x_1\ \ldots\ x_n}{t_1\ \ldots\ t_n}$ свободной для формулы $\mathcal{A}$, если для всех $i = 1, \ldots, n$ терм t_i свободен для переменной x_i в формуле $\mathcal{A}$. Выяснить, какие подстановки из примеров 1–3 на стр. 31 свободны для соответствующих формул.

§ 7. Примеры языков первого порядка

Языки первого порядка используются для записи математических утверждений, причем для каждой конкретной области математики, или, как говорят, математической теории, выбирается язык с подходящей сигнатурой. Использование языка первого порядка для записи утверждений, относящихся к данной математической теории, становится возможным, если удается расклассифицировать все основные понятия теории на «объекты», «функции» и «предикаты». При этом функции и предикаты должны быть определены

только на объектах, и значениями функций являются только объекты. В частности, не допускается рассматривать предикаты, заданные на функциях, или функции, заданные на предикатах. Затем для некоторых конкретных, замечательных в том или ином отношении объектов, функций и предикатов, мы фиксируем их обозначения, которые и образуют соответственно множества констант Cnst, функциональных символов Fn и предикатных символов Pr. Таким образом, возникает язык первого порядка с сигнатурой $\langle \mathrm{Cnst}, \mathrm{Fn}, \mathrm{Pr} \rangle$.

В математической логике разработаны языки для многих математических теорий. Рассмотрим два из них, играющих наиболее важную роль в логико-математических исследованиях.

1. Сигнатура *языка формальной арифметики* содержит единственную константу 0 и три функциональных символа: одноместный S и двуместные $+$ и $\cdot$. Условимся вместо $+(t_1, t_2)$ писать $t_1 + t_2$, а вместо $\cdot(t_1, t_2)$ — писать $t_1 \cdot t_2$. Подразумеваемый смысл символа S таков: $S(x) = x + 1$. Для краткости вместо $S(t)$ будем писать St. Имея в виду подразумеваемый смысл символов языка, можно ввести сокращенные обозначения для некоторых формул. Например, выражение $x \leqslant y$ будем считать сокращением для формулы $\exists z\ x + z = y$; $x < y$ — для формулы $\exists z\ x + Sz = y$; $x \vdots y$ — для $\exists z\ y \cdot z = x$.

2. Сигнатура *языка теории множеств* содержит только двуместный предикат символ $\in$. Условимся писать $t_1 \in t_2$ вместо $\in (t_1, t_2)$. Очевидно, что термами этого языка являются только переменные. Вот примеры формул языка теории множеств:

1) $\forall z\ (z \in x \supset z \in y)$. Имея в виду естественный подразумеваемый смысл символов языка, для этой формулы можно ввести сокращенное обозначение $x \subseteq y$.

2) $\neg x = y$. Ее можно было бы сокращенно обозначить $x \neq y$.

3) $\neg x \in y$. Эту формулу можно обозначить $x \notin y$.

4) $\neg \exists y\ y \in x$. Эту формулу естественно обозначить $x = \varnothing$.

§ 8. Определение интерпретации

При построении конкретного логико-математического языка обычно подразумевается некоторый смысл составляющих его символов, однако при описании языка, определении термов и формул этот смысл никак не используется. После того как выбрана сигнатура языка, мы вправе наделять входящие в нее символы новым смыслом, отличным от того, который вкладывался в них на этапе построения языка. Более того, рассмотрение различных интер-

претаций одного и того же языка является одним из важнейших приемов, используемых в математической логике, и именно с его помощью были получены многие важные результаты.

Чтобы задать *интерпретацию* сигнатуры $\Omega = \langle \mathrm{Cnst}, \mathrm{Fn}, \mathrm{Pr} \rangle$, нужно

1) фиксировать некоторое непустое множество M, называемое *носителем* интерпретации;

2) с каждой константой $c \in \mathrm{Cnst}$ сопоставить элемент $\overline{c} \in M$;

3) с каждым k-местным функциональным символом $f \in \mathrm{Fn}$ сопоставить некоторую k-местную функцию $\overline{f} : M^k \to M$;

4) с каждым k-местным предикатным символом $P \in \mathrm{Pr}$ сопоставить k-местный предикат $\overline{P} : M^k \to \{\text{И}, \text{Л}\}$.

Если P есть 0-местный предикатный символ, то с ним сопоставляется одно из двух истинностных значений И или Л.

Будем называть $\overline{c}$, $\overline{f}$, $\overline{P}$ интерпретациями соответственно константы c, функционального символа f и предикатного символа P.

Носитель интерпретации — множество M — объявляется областью возможных значений (или, что то же самое, областью изменения) для каждой переменной.

Пример 1. Пусть Ω — сигнатура языка формальной арифметики. Рассмотрим две интерпретации этой сигнатуры.

1) Носитель — множество натуральных чисел; $\overline{0}=0$, $\overline{S}(x)=x+1$, $\overline{+}(x,y)$ — сумма чисел x и y; $\overline{\cdot}(x,y)$ — произведение чисел x и y.

Здесь в соответствии с соглашением через $\overline{+}$, $\overline{\cdot}$, $\overline{S}$, $\overline{0}$ обозначены интерпретации символов $+$, $\cdot$, S, 0.

Мы употребили выражение «сумма чисел x и y» вместо более простого «$x+y$», чтобы не запутаться. Дело в том, что в равенстве $\overline{+}(x,y) = x+y$ знак $+$ используется в двух разных смыслах: слева от знака равенства он обозначает функциональный символ сигнатуры, который может иметь различные интерпретации, а справа от знака равенства знак $+$ есть имя функции сложения на натуральных числах. То же относится к знаку $\cdot$. В дальнейшем мы будем позволять себе использовать такие общеупотребительные знаки, как $=, <, +, \cdot$ в разных смыслах, не останавливаясь на разъяснениях.

Эта интерпретация называется *стандартной интерпретацией языка формальной арифметики.*

2) Носитель — множество натуральных чисел; $\overline{0} = 5$; $\overline{S}(x) = 2^x$; $\overline{\cdot}(x,y) = x + 2y$; $\overline{+}(x,y) = 2x + y$. Эта интерпретация не имеет названия, мы выбрали ее случайным образом.

Пример 2. Пусть сигнатура состоит из двух двуместных функциональных символов $+$ и $\cdot$. Тогда любое кольцо и любое поле является интерпретацией этой структуры.

Пример 3. Пусть сигнатура состоит из двуместного предикатного символа $<$. Любое упорядоченное множество является интерпретацией этой сигнатуры, если интерпретировать $<$ как предикат «быть меньше».

Разумеется, в этих примерах возможные интерпретации не исчерпываются приведенными.

Следует хорошо понимать различие между константами, функциональными символами, предикатными символами и их интерпретациями. Первые суть некоторые знаки, используемые при написании формул, а их интерпретации являются «настоящими» элементами, функциями и предикатами.

Упражнения.

1. В сигнатуре языка формальной арифметики записать формулу с одной свободной переменной x, истинную в стандартной интерпретации тогда и только тогда, когда

а) x четно;

б) $x \equiv 2 \pmod 3$;

в) x — простое число.

2. Записать замкнутую формулу в сигнатуре $\{P\}$, где P — двуместный предикатный символ, истинную в интерпретации I тогда и только тогда, когда носитель I линейно упорядочен отношением $\overline{P}$.

3. Пусть носитель интерпретации I сигнатуры $\{P\}$ есть множество всех подмножеств натуральных чисел, а $\overline{P}(x, y) =$ И означает, что $x \subseteq y$. Записать формулы, означающие $x = y \cap z$ и $x = y \cup z$.

§ 9. Формальное определение истинности

Если зафиксирована интерпретация данной сигнатуры, то каждая замкнутая формула этой сигнатуры превращается в высказывание, и с ней связывается ее истинностное значение И или Л.

Пример. Формулы

$$\forall x\ \forall y\ \exists z\ x + y = z, \qquad \exists y\ 0 = y \cdot SS0,$$
$$\forall x\ \forall y\ x \cdot Sy = x \cdot y + x, \qquad \exists x\ SSSS0 = x + x$$

истинны, а формулы

$$\forall x\ \forall y\ \forall z\ x + z = y, \qquad \exists y\ S0 = y \cdot SS0$$

ложны в стандартной интерпретации языка формальной арифметики.

Дадим более строгое, формальное определение истинностного значения замкнутой формулы. Пусть M — носитель интерпретации I сигнатуры $\Omega = \langle \mathrm{Cnst}, \mathrm{Fn}, \mathrm{Pr} \rangle$. С каждым элементом $m \in M$ сопоставим новую (т. е. не входящую в Cnst) константу $\underline{m}$ — имя элемента m. Через $\Omega(M)$ обозначим сигнатуру, полученную из Ω добавлением имен всех элементов из M в качестве констант, т. е. $\Omega(M) = \langle \mathrm{Cnst} \cup \{\underline{m} \mid m \in M\}, \mathrm{Fn}, \mathrm{Pr} \rangle$.

Подстановку вида $\begin{pmatrix} x_1 & \dots & x_n \\ \underline{a}_1 & \dots & \underline{a}_n \end{pmatrix}$, где $a_1, \dots, a_n \in M$, назовем *оценкой*. Будем говорить, что $\theta = \begin{pmatrix} x_1 & \dots & x_n \\ \underline{a}_1 & \dots & \underline{a}_n \end{pmatrix}$ — оценка терма (формулы) E, если E не содержит (свободных) вхождений переменных, отличных от $x_1, \dots, x_n$. Если θ — оценка терма (формулы) E, то θE будем называть *оцененным термом* (соответственно, *оцененной формулой*). Очевидно, что множество оцененных термов — это в точности множество всех термов языка $\Omega(M)$, не содержащих переменных, а множество оцененных формул — это множество всех замкнутых формул языка $\Omega(M)$.

Индукцией по построению оцененного терма t (т. е. терма языка $\Omega(M)$, не содержащего переменных) определим его значение, обозначаемое $|t|$. Это будет элемент множества M.

1) Если t есть константа $c \in \mathrm{Cnst}$, то $|t| = \overline{c}$. Если t есть константа $\underline{m}$, где $m \in M$, то $|t| = m$.

2) Если t имеет вид $f(t_1, \dots, t_n)$, где $t_1, \dots, t_n$ — оцененные термы, то $|t| = \overline{f}(|t_1|, \dots, |t_n|)$.

Теперь индукцией по количеству символов $\forall$, $\exists$, $\&$, $\neg$, $\vee$, $\supset$, $\equiv$ в оцененной формуле (т. е. в замкнутой формуле языка $\Omega(M)$) определим ее истинностное значение в интерпретации I. Достаточно определить, в каких случаях истинностное значение формулы равно И, и условиться, что в остальных случаях оно равно Л. Утверждение о том, что истинностное значение оцененной формулы $\mathcal{A}$ в интерпретации I есть И (Л), будем сокращенно записывать так: $I \models \mathcal{A}$ (соответственно, $I \not\models \mathcal{A}$).

1) Пусть $\mathcal{A}$ есть оцененная атомная формула вида $P(t_1, \dots, t_n)$. Тогда, очевидно, $t_1, \dots, t_n$ — оцененные термы. $I \models \mathcal{A}$ тогда и только тогда, когда $\overline{P}(|t_1|, \dots, |t_n|) = \text{И}$.

2) Пусть $\mathcal{A}$ есть оцененная атомная формула вида $t_1 = t_2$. Тогда t_1 и t_2 — оцененные термы. $I \models \mathcal{A}$ тогда и только тогда, когда $|t_1| = |t_2|$.

3) Пусть $\mathcal{A}$ имеет вид $\neg\mathcal{B}$. Тогда $\mathcal{B}$ — оцененная формула. $I \models \mathcal{A}$ тогда и только тогда, когда $I \not\models \mathcal{B}$.

Пусть $\mathcal{A}$ имеет вид $(\mathcal{B} \,\&\, \mathcal{C})$, $(\mathcal{B} \vee \mathcal{C})$, $(\mathcal{B} \supset \mathcal{C})$ или $(\mathcal{B} \equiv \mathcal{C})$. Тогда $\mathcal{B}$ и $\mathcal{C}$ — оцененные формулы.

4) $I \models (\mathcal{B} \,\&\, \mathcal{C})$ тогда и только тогда, когда $I \models \mathcal{B}$ и $I \models \mathcal{C}$.

5) $I \models (\mathcal{B} \vee \mathcal{C})$ тогда и только тогда, когда $I \models \mathcal{B}$ или $I \models \mathcal{C}$.

6) $I \models (\mathcal{B} \supset \mathcal{C})$ тогда и только тогда, когда $I \not\models \mathcal{B}$ или $I \models \mathcal{C}$.

7) $I \models (\mathcal{B} \equiv \mathcal{C})$ тогда и только тогда, когда истинностные значения формул $\mathcal{B}$ и $\mathcal{C}$ в интерпретации I совпадают.

Пусть $\mathcal{A}$ имеет вид $\exists x\ \mathcal{B}(x)$ или $\forall x\ \mathcal{B}(x)$. Тогда $\mathcal{B}(\underline{a})$ является оцененной формулой при любом $a \in M$.

8) $I \models \exists x\ \mathcal{B}(x)$ тогда и только тогда, когда существует такой элемент $a \in M$, что $I \models \mathcal{B}(\underline{a})$.

9) $I \models \forall x\ \mathcal{B}(x)$ тогда и только тогда, когда $I \models \mathcal{B}(\underline{a})$ для всех $a \in M$.

Мы определили отношение $I \models \mathcal{A}$ для произвольной оцененной формулы $\mathcal{A}$. Очевидно, что любая замкнутая формула языка Ω является оцененной формулой. Поэтому приведенное определение с каждой такой формулой сопоставляет ее истинностное значение в интерпретации I.

§ 10. Общезначимые формулы, выполнимые формулы, равносильные формулы

Формула называется *общезначимой* (или *тождественно истинной*), если она истинна в любой интерпретации при любой ее оценке.

Пример 1. Докажем, что формула $\exists x\, \forall y\ P(x,y) \supset \forall y\, \exists x\ P(x,y)$ общезначима. Обозначим ее через $\mathcal{A}$. Пусть I — произвольная интерпретация, M — ее носитель. Если $I \not\models \exists x\ \forall y\ P(x,y)$, то $I \models \mathcal{A}$, как видно из пункта 6) определения истинности. Рассмотрим случай, когда $I \models \exists x\ \forall y\ P(x,y)$. По пункту 8) определения истинности найдется $m \in M$, для которого $I \models \forall y\ P(\underline{m},y)$. Тогда по пункту 9) определения истинности $I \models P(\underline{m},\underline{n})$ для всех $n \in M$. Значит, по пункту 8) того же определения $I \models \exists x\ P(x,\underline{n})$ для всех $n \in M$, а по пункту 9) $I \models \forall y\ \exists x\ P(x,y)$. По пункту 6) определения истинности это означает, что $I \models \mathcal{A}$.

В § 3 главы 2 было введено понятие тавтологии как пропозициональной формулы, которая превращается в истинное высказывание при любой подстановке в нее конкретных высказываний вместо пропозициональных переменных. Распространим понятие тавтологии на формулы языка первого порядка.

Очевидно, что если в пропозициональную формулу вместо всех пропозициональных переменных подставить какие-нибудь формулы языка первого порядка, то получится формула языка первого порядка. Пусть $\mathcal{B}(P_1, \dots, P_n)$ — пропозициональная формула с пропозициональными переменными $P_1, \dots, P_n$, а $\mathcal{A}_1, \dots, \mathcal{A}_n$ — произвольные формулы языка первого порядка. Обозначим через $\mathcal{B}(\mathcal{A}_1, \dots, \mathcal{A}_n)$ формулу, полученную подстановкой в $\mathcal{B}(P_1, \dots, P_n)$ формул $\mathcal{A}_1, \dots, \mathcal{A}_n$ вместо $P_1, \dots, P_n$ соответственно.

Формула $\mathcal{A}$ языка первого порядка называется *тавтологией*, если существуют такая пропозициональная тавтология $\mathcal{B}(P_1, \dots, P_n)$ и такие формулы языка первого порядка $\mathcal{A}_1, \dots, \mathcal{A}_n$, что $\mathcal{A}$ есть $\mathcal{B}(\mathcal{A}_1, \dots, \mathcal{A}_n)$.

Пример 2. Формула $\forall x\; R(x) \vee \neg\forall x\; R(x)$ является тавтологией. Она получается из пропозициональной тавтологии $P \vee \neg P$ подстановкой $\forall x\; R(x)$ вместо P.

Пример 3. Формула $\exists y\; Q(y) \;\&\; (\exists y\; Q(y) \supset R(z)) \supset R(z)$ также является тавтологией. Она получается из пропозициональной тавтологии $P_1 \;\&\; (P_1 \supset P_2) \supset P_2$ подстановкой $\exists y\; Q(y)$ вместо P_1 и R(z) вместо P_2.

Теорема 1. *Любая тавтология общезначима.*

Доказательство. В дальнейшем мы будем употреблять знак «графического равенства» $\doteq$ для выражения одинаковости слов: $A \doteq B$ означает, что слова A и B одинаковы, т. е. построены из одинаковых букв, расположенных в одинаковом порядке.

Пусть $\mathcal{A}$ — формула языка Ω, являющаяся тавтологией. Это означает, что $\mathcal{A} \doteq \mathcal{B}(\mathcal{A}_1, \dots, \mathcal{A}_n)$ для некоторой пропозициональной тавтологии $\mathcal{B}(P_1, \dots, P_n)$ и формул $\mathcal{A}_1, \dots, \mathcal{A}_n$ языка Ω. Пусть I — произвольная интерпретация, θ — произвольная оценка формулы $\mathcal{A}$. Очевидно, что $\theta\mathcal{A} \doteq \mathcal{B}(\theta\mathcal{A}_1, \dots, \theta\mathcal{A}_n)$. Поэтому вычисление истинностного значения формулы $\mathcal{A}$ по существу состоит в вычислении значения, которое примет формула $\mathcal{B}(P_1, \dots, P_n)$ при подстановке в нее истинностных значений формул $\theta\mathcal{A}_1, \dots, \theta\mathcal{A}_n$ вместо $P_1, \dots, P_n$. Поскольку $\mathcal{B}(P_1, \dots, P_n)$ — тавтология, она всегда

принимает значение И. Значит, $I \models \theta\mathcal{A}$. Таким образом, формула $\mathcal{A}$ истинна в любой интерпретации при любой оценке, т. е. она общезначима. Теорема 1 доказана.

Формула называется *выполнимой*, если она истинна хотя бы в одной интерпретации при хотя бы одной ее оценке.

Пример 4. Формула $\exists x\ \exists y\ (P(x) \,\&\, \neg P(y))$ выполнима, но не общезначима. Обозначим эту формулу через $\mathcal{A}$. Возьмем в качестве носителя интерпретации множество $\{0, 1\}$ и положим $\overline{P}(0) =$ И, $\overline{P}(1) =$ Л. Нетрудно видеть, что в этой интерпретации формула $\mathcal{A}$ ложна, следовательно, она не общезначима.

Формулы $\mathcal{A}$ и $\mathcal{B}$ называются *равносильными*, если формула $(\mathcal{A} \equiv \mathcal{B})$ общезначима. Если $\mathcal{A}$ и $\mathcal{B}$ равносильны, будем писать $\mathcal{A} \sim \mathcal{B}$.

Теорема 2. *Каковы бы ни были формулы $\mathcal{A}$ и $\mathcal{B}$, справедливы следующие утверждения о равносильности*:

1. *Если $\mathcal{B}$ не содержит свободных вхождений переменной x, то*
   а) $\exists x\ (\mathcal{A} \,\&\, \mathcal{B}) \sim \exists x\ \mathcal{A} \,\&\, \mathcal{B}$;
   б) $\forall x\ (\mathcal{A} \,\&\, \mathcal{B}) \sim \forall x\ \mathcal{A} \,\&\, \mathcal{B}$;
   в) $\forall x\ (\mathcal{A} \vee \mathcal{B}) \sim \forall x\ \mathcal{A} \vee \mathcal{B}$;
   г) $\exists x\ (\mathcal{A} \vee \mathcal{B}) \sim \exists x\ \mathcal{A} \vee \mathcal{B}$;
2. $\exists x\ (\mathcal{A} \vee \mathcal{B}) \sim \exists x\ \mathcal{A} \vee \exists x\ \mathcal{B}$;
3. $\forall x\ (\mathcal{A} \,\&\, \mathcal{B}) \sim \forall x\ \mathcal{A} \,\&\, \forall x\ \mathcal{B}$;
4. $\neg\exists x\ \mathcal{A} \sim \forall x\ \neg\mathcal{A}$;
5. $\neg\forall x\ \mathcal{A} \sim \exists x\ \neg\mathcal{A}$;
6. *если $\mathcal{A}(x)$ не содержит y, то*
   а) $\forall x\ \mathcal{A}(x) \sim \forall y\ \mathcal{A}(y)$;
   б) $\exists x\ \mathcal{A}(x) \sim \exists y\ \mathcal{A}(y)$.

Доказательство. Мы докажем только равносильности 1.в) и 2. Доказательство остальных равносильностей проводится по тому же образцу и предлагается в качестве упражнения.

Итак, докажем, что $\forall x\ (\mathcal{A} \vee \mathcal{B}) \sim \forall x\ \mathcal{A} \vee \mathcal{B}$, т. е. что формула $\forall x\ (\mathcal{A} \vee \mathcal{B}) \equiv (\forall x\ \mathcal{A} \vee \mathcal{B})$, которую мы обозначим через $\mathcal{C}$, общезначима, если $\mathcal{B}$ не содержит свободных вхождений x. Пусть I — произвольная интерпретация, M — ее носитель, θ — произвольная оценка формулы $\mathcal{C}$. Надо доказать, что $I \models \theta\mathcal{C}$.

Переменная x не имеет свободных вхождений в $\mathcal{C}$. Поэтому формула $\theta\mathcal{C}$ не зависит от того, какой терм подставляется при оценке θ вместо переменной x, и можно считать, что оценка θ вообще не содержит x.

Очевидно, что $\theta\mathcal{C} \doteq \forall x\ (\theta\mathcal{A} \vee \theta\mathcal{B}) \equiv (\forall x\ \theta\mathcal{A} \vee \mathcal{B})$. Формулу $\forall x\ (\theta\mathcal{A} \vee \theta\mathcal{B})$ обозначим через $\mathcal{C}_1$, а $(\forall x\ \theta\mathcal{A} \vee \mathcal{B})$ — через $\mathcal{C}_2$. Заметим, что формула $\theta\mathcal{A}$ может содержать свободные вхождения переменной x, поэтому для нее будем употреблять обозначение $\theta\mathcal{A}(x)$. Формула же $\theta\mathcal{B}$ замкнута, следовательно, либо $I \models \theta\mathcal{B}$, либо $I \not\models \theta\mathcal{B}$. Пусть $I \models \theta\mathcal{B}$. Тогда, по пункту 5) определения истинности, $I \models \forall x\ \theta\mathcal{A} \vee \mathcal{B}$, т. е. $I \models \mathcal{C}_2$, и $I \models \theta\mathcal{A}(\underline{m}) \vee \mathcal{B}$ для всех $m \in M$, значит, $I \models \forall x\ (\theta\mathcal{A} \vee \mathcal{B})$, т. е. $I \models \mathcal{C}_1$. Значит, $\mathcal{C}_1$ и $\mathcal{C}_2$ обе истинны, и $I \models \theta\mathcal{C}$. Пусть $I \not\models \theta\mathcal{B}$. Тогда, очевидно, какова бы ни была замкнутая формула $\mathcal{F}$, истинностные значения формул $\mathcal{F} \vee \theta\mathcal{B}$ и $\mathcal{F}$ совпадают. Поэтому $I \models \forall x\ (\theta\mathcal{A}(x) \vee \theta\mathcal{B}) \Leftrightarrow I \models \theta\mathcal{A}(\underline{m}) \vee \theta\mathcal{B}$ для всех $m \in M \Leftrightarrow I \models \theta\mathcal{A}(\underline{m})$ для всех $m \in M \Leftrightarrow I \models \forall x\ \theta\mathcal{A} \Leftrightarrow I \models \forall x\ \theta\mathcal{A} \vee \theta\mathcal{B}$. Таким образом, $I \models \mathcal{C}_1 \Leftrightarrow I \models \mathcal{C}_2$, т. е. $I \models \theta\mathcal{C}$. Равносильность 1 в) доказана.

Докажем равносильность 2. Требуется доказать общезначимость формулы $\exists x\ (\mathcal{A} \vee \mathcal{B}) \equiv (\exists x\ \mathcal{A} \vee \exists x\ \mathcal{B})$, которую мы обозначим $\mathcal{D}$.

Пусть I — произвольная интерпретация, M — ее носитель, θ — произвольная оценка формулы $\mathcal{D}$. Так как $\mathcal{D}$ не содержит свободных вхождений x, можно считать, что x не входит в θ. Имеем $\theta\mathcal{D} \doteq \exists x\ (\theta\mathcal{A} \vee \theta\mathcal{B}) \equiv (\exists x\ \theta\mathcal{A} \vee \exists x\ \theta\mathcal{B})$. Докажем, что $I \models \exists x\ (\theta\mathcal{A} \vee \theta\mathcal{B}) \Leftrightarrow I \models (\exists x\ \theta\mathcal{A} \vee \exists x\ \theta\mathcal{B})$. Формулы $\theta\mathcal{A}$ и $\theta\mathcal{B}$ могут содержать свободные вхождения x, поэтому будем употреблять для них обозначения $\theta\mathcal{A}(x)$ и $\theta\mathcal{B}(x)$. Имеем $I \models \exists x\ (\theta\mathcal{A} \vee \theta\mathcal{B}) \Leftrightarrow I \models (\theta\mathcal{A}(\underline{m}) \vee \theta\mathcal{B}(\underline{m}))$ для некоторого $m \in M \Leftrightarrow I \models \theta\mathcal{A}(\underline{m})$ или $I \models \theta\mathcal{B}(\underline{m})$ для некоторого $m \in M \Leftrightarrow I \models \exists x\ \theta\mathcal{A}$ или $I \models \exists x\ \theta\mathcal{B} \Leftrightarrow I \models \exists x\ \theta\mathcal{A} \vee \exists x\ \theta\mathcal{B}$, что и требовалось доказать. Теорема доказана.

Теорема 3. *Пусть $\mathcal{A}$ — произвольная формула, а $\mathcal{B}$ и $\mathcal{B}_1$ — равносильные формулы. Тогда*

1) $(\mathcal{A} \,\&\, \mathcal{B}) \sim (\mathcal{A} \,\&\, \mathcal{B}_1)$;
2) $(\mathcal{A} \vee \mathcal{B}) \sim (\mathcal{A} \vee \mathcal{B}_1)$;
3) $(\mathcal{A} \supset \mathcal{B}) \sim (\mathcal{A} \supset \mathcal{B}_1)$;
4) $(\mathcal{B} \supset \mathcal{A}) \sim (\mathcal{B}_1 \supset \mathcal{A})$;
5) $(\mathcal{A} \equiv \mathcal{B}) \sim (\mathcal{A} \equiv \mathcal{B}_1)$;
6) $\neg\mathcal{B} \sim \neg\mathcal{B}_1$;
7) $\exists x\ \mathcal{B} \sim \exists x\ \mathcal{B}_1$;
8) $\forall x\ \mathcal{B} \sim \forall x\ \mathcal{B}_1$.

Доказательство. Утверждения 1)–6) немедленно следуют из определения истинности. Докажем 7). Утверждение 8) доказывается аналогично и предлагается в качестве упражнения.

Итак, требуется доказать, что формула $(\exists x\ \mathcal{B} \equiv \exists x\ \mathcal{B}_1)$ общезначима. Пусть I — произвольная интерпретация, M — ее носитель. Пусть θ — произвольная оценка формулы $(\exists x\ \mathcal{B} \equiv \exists x\ \mathcal{B}_1)$. Так как эта формула не содержит свободных вхождений x, можно считать, что x не входит в θ. Имеем $\theta(\exists x\ \mathcal{B} \equiv \exists x\ \mathcal{B}_1) \doteq (\exists x\ \theta\mathcal{B} \equiv \exists x\ \theta\mathcal{B}_1)$. Так как $\theta\mathcal{B}$ и $\theta\mathcal{B}_1$ могут содержать свободные вхождения перемен-

ной x, будем для них употреблять обозначения $\theta\mathcal{B}(x)$ и $\theta\mathcal{B}_1(x)$. Докажем, что $I \models \exists x\ \theta\mathcal{B}(x) \Leftrightarrow I \models \exists x\ \mathcal{B}_1(x)$. Пусть $I \models \exists x\ \theta\mathcal{B}(x)$. Тогда найдется такой элемент $m \in M$, что $I \models \theta\mathcal{B}(\underline{m})$. По условию, $\mathcal{B} \sim \mathcal{B}_1$. Значит, $I \models \theta'(\mathcal{B} \equiv \mathcal{B}_1)$, где θ' — оценка, полученная из θ добавлением подстановки $\underline{m}$ вместо x. Но $\theta'(\mathcal{B} \equiv \mathcal{B}_1) \doteqdot (\theta'\mathcal{B} \equiv \theta'\mathcal{B}_1) \doteqdot (\theta\mathcal{B}(\underline{m}) \equiv \theta\mathcal{B}_1(\underline{m}))$. Таким образом, $I \models (\theta\mathcal{B}(\underline{m}) \equiv \theta\mathcal{B}_1(\underline{m}))$. Учитывая, что $I \models \theta\mathcal{B}(\underline{m})$, отсюда получаем $I \models \theta\mathcal{B}_1(\underline{m})$ и $I \models \exists x\ \theta\mathcal{B}_1$. Аналогично доказывается, что если $I \models \exists x\ \theta\mathcal{B}_1(x)$, то $I \models \exists x\ \theta\mathcal{B}(x)$. Из доказанного следует $I \models \exists x\ \theta\mathcal{B} \equiv \exists x\ \theta\mathcal{B}_1$, т.е. $I \models \theta(\exists x\ \mathcal{B} \equiv \exists x\ \mathcal{B}_1)$. Таким образом, формула $\exists x\ \mathcal{B} \equiv \exists x\ \mathcal{B}_1$ истинна в любой интерпретации при любой оценке. Значит, она общезначима. Теорема 3 доказана.

Теорема 4. *Если $\mathcal{A} \sim \mathcal{B}$ и $\mathcal{B} \sim \mathcal{C}$, то $\mathcal{A} \sim \mathcal{C}$.*

Это утверждение очевидно.

Теорема 5. *Пусть $\mathcal{B}$ и $\mathcal{B}_1$ — равносильные формулы, а $\mathcal{A}$ — произвольная формула. Пусть $\mathcal{A}_1$ получена из $\mathcal{A}$ заменой некоторых вхождений формулы $\mathcal{B}$ на $\mathcal{B}_1$. Тогда $\mathcal{A} \sim \mathcal{A}_1$.*

Доказательство. Утверждение несложно доказывается индукцией по построению формулы $\mathcal{A}$ с помощью теорем 3 и 4.

Теорема 6. *Любая формула равносильна некоторой формуле, не содержащей связок $\&, \supset, \equiv$ и квантора $\forall$.*

Доказательство. Докажем теорему индукцией по построению формулы.

1) Пусть $\mathcal{A}$ — атомная формула. Тогда $\mathcal{A}$ не содержит символов $\&, \supset, \equiv, \forall$.

2) Пусть $\mathcal{A}$ имеет вид $(\mathcal{A}_1 \ \&\ \mathcal{A}_2)$. По индуктивному предположению $\mathcal{A}_1 \sim \mathcal{B}_1$, $\mathcal{A}_2 \sim \mathcal{B}_2$, где $\mathcal{B}_1$ и $\mathcal{B}_2$ не содержат $\&, \supset, \equiv, \forall$. Используем очевидную равносильность

$$\mathcal{A} \,\&\, \mathcal{B} \sim \neg(\neg\mathcal{A} \vee \neg\mathcal{B}).$$

Тогда по теоремам 4 и 5

$$\mathcal{A} \doteqdot (\mathcal{A}_1 \ \&\ \mathcal{A}_2) \sim \neg(\neg\mathcal{A}_1 \vee \neg\mathcal{A}_2) \sim \neg(\neg\mathcal{B}_1 \vee \neg\mathcal{B}_2).$$

Последняя формула не содержит $\&, \supset, \equiv, \forall$.

Аналогично разбираются случаи $\mathcal{A} \rightleftharpoons \neg\mathcal{A}_1$; $\mathcal{A} \rightleftharpoons (\mathcal{A}_1 \vee \mathcal{A}_2)$; $\mathcal{A} \rightleftharpoons (\mathcal{A}_1 \supset \mathcal{A}_2)$; $\mathcal{A} \rightleftharpoons (\mathcal{A}_1 \equiv \mathcal{A}_2)$; $\mathcal{A} \rightleftharpoons \forall x\ \mathcal{A}_1$; $\mathcal{A} \rightleftharpoons \exists x\ \mathcal{A}_1$. При этом используются следующие равносильности:

$$\mathcal{A} \supset \mathcal{B} \sim \neg\mathcal{A} \vee \mathcal{B};$$
$$\mathcal{A} \equiv \mathcal{B} \sim (\mathcal{A} \supset \mathcal{B})\ \&\ (\mathcal{B} \supset \mathcal{A}) \sim \neg(\neg(\neg\mathcal{A} \vee \mathcal{B}) \vee \neg(\neg\mathcal{B} \vee \mathcal{A}));$$
$$\forall x\ \mathcal{A} \sim \neg\exists x\ \neg\mathcal{A}.$$

Упражнения.

1. Доказать, что формула $\mathcal{A}$ общезначима тогда и только тогда, когда $\neg\mathcal{A}$ не выполнима.

2. Выполнимы ли следующие формулы:

а) $\exists x\ P(x)$;

б) $\forall x\ P(x)$;

в) $\exists x\ \forall y\ (Q(x,x)\ \&\ \neg Q(x,y))$;

г) $\exists x\ \forall y\ (Q(x,y) \supset \forall z\ R(x,y,z))$?

3. Являются ли общезначимыми следующие формулы:

а) $\exists x\ P(x) \supset \forall x\ P(x)$;

б) $\neg(\exists x\ P(x) \supset \forall x\ P(x))$;

в) $\forall x\ \exists y\ Q(x,y) \supset \exists y\ \forall x\ Q(x,y)$?

4. Пусть $\mathcal{A}(x)$ — формула без кванторов и функциональных символов с единственной переменной x такая, что формула $\exists x\ \mathcal{A}(x)$ общезначима. Доказать, что для некоторых констант $c_1, \ldots, c_n$ формула $\mathcal{A}(c_1) \vee \ldots \vee \mathcal{A}(c_n)$ общезначима.

5. Равносильны ли формулы $P(x)$ и $\forall x\ P(x)$?

§ 11. Предваренные формулы

Формулу $\mathcal{A}$ будем называть *предваренной формулой*, если $\mathcal{A}$ имеет вид $Q_1x_1Q_2x_2\ldots Q_nx_n\mathcal{B}$, где $Q_1, Q_2, \ldots, Q_n$ — кванторы, а формула $\mathcal{B}$ не содержит кванторов.

Теорема 7. *Каждая формула равносильна некоторой предваренной формуле.*

Доказательство. Пусть $\mathcal{A}$ — произвольная формула. По теореме 6 любая формула эквивалентна формуле, не содержащей $\&, \supset, \equiv$. Докажем теорему индукцией по построению $\mathcal{A}$.

1) Пусть $\mathcal{A}$ — атомная формула. Тогда $\mathcal{A}$ сама является предваренной формулой.

2) Пусть $\mathcal{A} \rightleftharpoons \neg\mathcal{B}$. По индуктивному предположению

$$\mathcal{B} \sim Q_1x_1 \dots Q_nx_n\mathcal{D},$$

где $\mathcal{D}$ — бескванторная формула. Тогда

$$\mathcal{A} \sim \neg Q_1x_1 \dots Q_nx_n\mathcal{D} \sim \overline{Q}_1x_1 \dots \overline{Q}_nx_n\neg\mathcal{D},$$

где

$$\overline{Q}_i = \begin{cases} \forall, & \text{если } Q_i \rightleftharpoons \exists; \\ \exists, & \text{если } Q_i \rightleftharpoons \forall. \end{cases}$$

3) Пусть $\mathcal{A}$ имеет вид $(\mathcal{B}_1 \vee \mathcal{B}_2)$. По индуктивному предложению $\mathcal{B}_1 \sim Q_1x_1 \dots Q_nx_n\mathcal{D}_1$, $\mathcal{B}_2 \sim Q'_1y_1 \dots Q'_my_m\mathcal{D}_2$, где $\mathcal{D}_1$ и $\mathcal{D}_2$ — бескванторные формулы.

Выберем переменные $z_1, \dots, z_n$ по следующему правилу: если x_i не входит в $\mathcal{D}_2$, то $z_i \rightleftharpoons x_i$; если же x_i входит в $\mathcal{D}_2$, то в качестве z_i возьмем какую-нибудь переменную, не входящую в $\mathcal{D}_1$ и $\mathcal{D}_2$. При этом должно соблюдаться условие: $z_i \rightleftharpoons z_j$ тогда и только тогда, когда $x_i \rightleftharpoons x_j$. Обозначим через $\mathcal{C}_1$ формулу, полученную из $\mathcal{D}_1$ заменой переменных $x_1, \dots, x_n$ на $z_1, \dots, z_n$ соответственно. Тогда $Q_1x_1 \dots Q_nx_n\mathcal{D}_1 \sim Q_1z_1 \dots Q_nz_n\mathcal{C}_1$. Для доказательства этого достаточно n раз воспользоваться равносильностями 6.а) и 6.б) из теоремы 2.

Ту же операцию проделаем с формулой $Q'_1y_1 \dots Q'_my_m\mathcal{D}_2$. А именно, выберем переменные $u_1, \dots, u_m$ так, что если y_i не входит в $\mathcal{C}_1$, то $u_i \rightleftharpoons y_i$, а если y_i входит в $\mathcal{C}_1$, то u_i — какая-нибудь переменная, не входящая в $\mathcal{D}_2$ и $\mathcal{C}_1$, причем $u_i \rightleftharpoons u_j$ тогда и только тогда, когда $y_i \rightleftharpoons y_j$. Через $\mathcal{C}_2$ обозначим формулу, полученную из $\mathcal{D}_2$ заменой $y_1, \dots, y_m$ на $u_1, \dots, u_m$ соответственно. Тогда $Q'_1y_1 \dots Q'_my_m\mathcal{D}_2 \sim Q'_1u_1 \dots Q'_mu_m\mathcal{C}_2$.

Теперь

$$\mathcal{B}_1 \vee \mathcal{B}_2 \sim Q_1z_1 \dots Q_nz_n\mathcal{C}_1 \vee Q'_1u_1 \dots Q'_mu_m\mathcal{C}_2 \sim$$
$$\sim Q_1z_1 \dots Q_nz_nQ'_1u_1 \dots Q'_mu_m(\mathcal{C}_1 \vee \mathcal{C}_2)$$

(мы использовали $n + m$ раз равносильности 1.в) и 1.г) из теоремы 2; замена переменных сделана именно для того,чтобы можно было воспользоваться этими равносильностями).

4) Пусть $\mathcal{A} \rightleftharpoons Qx\mathcal{B}$, где Q — это квантор $\exists$ или $\forall$. По индуктивному предложению $\mathcal{B} \sim Q_1x_1 \dots Q_mx_m\mathcal{D}$, где $\mathcal{D}$ — бескванторная формула. Тогда $\mathcal{A} \sim QxQ_1x_1 \dots Q_mx_m\mathcal{D}$.

Поскольку любая формула без символов $\supset, \equiv, \&$ имеет один из разобранных видов, теорема доказана.

В приведении данной формулы к предваренной форме (т. е. в построении предваренной формулы, равносильной данной) не обязательно следовать доказательству теоремы 7. Например, можно не избавляться от символов $\supset$ и $\&$, а использовать равносильности

$$(\forall x\ \mathcal{A} \supset \mathcal{B}) \sim \exists x\ (\mathcal{A} \supset \mathcal{B});$$
$$(\exists x\ \mathcal{A} \supset \mathcal{B}) \sim \forall x\ (\mathcal{A} \supset \mathcal{B});$$
$$(\mathcal{B} \supset \forall x\ \mathcal{A}) \sim \forall x\ (\mathcal{B} \supset \mathcal{A});$$
$$(\mathcal{B} \supset \exists x\ \mathcal{A}) \sim \exists x\ (\mathcal{B} \supset \mathcal{A})$$

(всюду переменная x не является свободной в $\mathcal{B}$) и равносильности 1.а) и 1.б) из теоремы 2.

Пример. Приведем формулу

$$\forall x\ P(x) \,\&\, \exists y\ Q(y) \supset \exists z\ R(y, z)$$

к предваренной форме:

$$\forall x\ P(x) \,\&\, \exists y\ Q(y) \sim \forall x\ \exists y\ (P(x) \,\&\, Q(y));$$
$$\forall x\ \exists y\ (P(x) \,\&\, Q(y)) \supset \exists z\ R(y, z) \sim$$
$$\sim \forall x\ \exists u\ (P(x) \,\&\, Q(u)) \supset \exists z\ R(y, z) \sim$$
$$\sim \exists x\ \forall u\ \exists z\ (P(x) \,\&\, Q(u) \supset R(y, z)).$$

Таким образом,

$$\forall x\ P(x) \,\&\, \exists y\ Q(y) \supset \exists z\ R(y, z) \sim \exists x\ \forall u\ \exists z\ (P(x) \,\&\, Q(u) \supset R(y, z)).$$

§ 12. Истинность в конечных интерпретациях

Пусть k — положительное натуральное число. Формула $\mathcal{A}$ называется *k-общезначимой*, если $\mathcal{A}$ истинна во всех интерпретациях с носителем из k элементов при любой оценке. Формула называется *конечно-общезначимой*, если она истинна во всех интерпретациях с конечным носителем при любой оценке. Очевидно, что любая общезначимая формула является k-общезначимой для любого k, т. е. конечно-общезначимой.

Пример. Формула $\exists x\, P(x) \supset \forall x\, P(x)$ является 1-общезначимой, но не общезначимой.

Теорема 8. *Для каждого $k \geqslant 1$ существует*

а) формула F_k, истинная в точности во всех интерпретациях с не более чем k-элементным носителем;

б) формула G_k, истинная в точности во всех интерпретациях с не менее чем k-элементным носителем;

в) формула E_k, истинная в точности во всех интерпретациях с k-элементным носителем.

Доказательство. а) Положим

$$F_k \rightleftharpoons \exists x_1\ \exists x_2\ \ldots \exists x_k\ \forall y\ (y = x_1 \lor y = x_2 \lor \ldots \lor y = x_k).$$

б) Положим

$$G_k \rightleftharpoons \exists x_1\ \ldots \exists x_k\ (\neg x_1 = x_2 \,\&\, \neg x_1 = x_3 \,\&\, \ldots \,\&\, \neg x_{k-1} = x_k)$$

(в бескванторную часть G_k входят формулы $\neg x_i = x_j$ при $i < j$).

в) Положим $E_k \rightleftharpoons F_k \,\&\, G_k$.

Теорема 8 доказана.

Теорема 9. *Существует конечно-общезначимая, но не общезначимая формула.*

Доказательство. Такова формула

$$\neg(\forall x\ \forall y\ \forall z\ (P(x,y) \,\&\, P(y,z) \supset P(x,z)) \,\&\\ \&\, \forall x\ \neg P(x,x) \,\&\, \forall x\ \exists y\ P(x,y)).$$

Действительно, она не общезначима, так как ложна в следующей интерпретации: носитель — множество натуральных чисел; $\overline{P}(x,y) = \text{И}$ тогда и только тогда, когда $x < y$.

Докажем, что эта формула конечно-общезначима. Пусть I — какая-нибудь интепретация с конечным носителем M, в которой рассматриваемая формула ложна, т. е. истинна формула

$$\forall x\ \forall y\ \forall z\ (P(x,y) \,\&\, P(y,z) \supset P(x,z)) \,\&\\ \&\, \forall x\ \neg P(x,x) \,\&\, \forall x\ \exists y\ P(x,y).$$

Тогда предикат $\overline{P}(x,y)$ определяет строгое частичное упорядочение на M в следующем смысле. Для $a, b \in M$ положим $a < b$, если

$\overline{P}(a,b) =$ И. Так как $I \models \forall x\ \forall y\ \forall z\ (P(x,y)\ \&\ P(y,z) \supset P(x,z))$, отношение $<$ транзитивно, и так как $I \models \forall x\ \neg P(x,x)$, отношение $<$ иррефлексивно. Но любое конечное частично упорядоченное множество имеет максимальный элемент, т. е. такой элемент a, что для всех $b \in M$ неверно, что $a < b$. Получаем противоречие, так как $I \models \forall x\ \exists y\ P(x,y)$.

Теорема 9 доказана.

Упражнения.

1. Доказать, что формула

$$\exists x\ \forall y\ (P(x,y) \supset (\neg P(y,x) \supset (P(x,x) \equiv P(y,y))))$$

3-общезначима.

2. Доказать, что следующие формулы конечно-общезначимы, но не общезначимы:

а) $\exists x\ \forall y\ \exists z\ ((P(y,z) \supset P(x,z)) \supset (P(x,x) \supset P(y,x)))$;

б) $\forall x\ \forall y\ \forall z\ (P(x,x) \& (P(x,z) \supset (P(x,y) \vee P(y,z))) \supset \exists y\ \forall z\ P(y,z)$.

3. Доказать, что формула сигнатуры $\{P_1, \ldots, P_n\}$, где $P_1, \ldots \ldots, P_n$ — одноместные предикатные символы, общезначима тогда и только тогда, когда она истинна во всех интерпретациях с 2^n-элементным носителем.

4. Для каждого натурального числа $k \geqslant 1$ построить формулу в сигнатуре из одноместных предикатных символов, не содержащую знака $=$, которая i-общезначима при всех $i < k$, но не k-общезначима.

§ 13. Изоморфизмы и элементарная эквивалентность

Пусть $\Omega = \langle \mathrm{Cnst}, \mathrm{Fn}, \mathrm{Pr} \rangle$ — некоторая сигнатура, I_1, I_2 — две ее интерпретации. Обозначим носитель I_1 через M_1, носитель I_2 — через M_2. Интерпретации константы c, функционального символа f и предикатного символа P в I_1 обозначим соответственно $\overline{c}, \overline{f}, \overline{P}$, а в I_2 — соответственно $\widetilde{c}, \widetilde{f}, \widetilde{P}$.

Пусть φ — некоторая функция из M_1 в M_2. Вместо $\varphi(m)$ для краткости будем писать φm. Будем говорить, что φ *сохраняет константу* c, если $\varphi\overline{c} = \widetilde{c}$; φ *сохраняет функциональный символ* f, если для всех $a_1, \ldots, a_n \in M_1$ выполнено $\varphi\overline{f}(a_1, \ldots, a_n) = \widetilde{f}(\varphi a_1, \ldots, \varphi a_n)$; φ *сохраняет предикатный символ* P, если для всех $a_1, \ldots, a_n \in M_1$ выполнено $\overline{P}(a_1, \ldots, a_n) = \widetilde{P}(\varphi a_1, \ldots, \varphi a_n)$. Функция φ называется

изоморфизмом из I_1 в I_2, если 1) φ — биекция, т. е. взаимно однозначное соответствие между множествами M_1 и M_2; 2) φ сохраняет все константы, все предикатные символы и все функциональные символы сигнатуры Ω. Интерпретация I_1 *изоморфна* интерпретации I_2, если существует изоморфизм из I_1 в I_2. Изоморфность интерпретаций I_1 и I_2 будем обозначать $I_1 \simeq I_2$.

Нетрудно видеть, что приведенное понятие изоморфизма является обобщением используемого в алгебре понятия изоморфизма групп, колец, полей и других алгебраических структур, которые можно рассматривать как интерпретации подходящих сигнатур.

Пример 1. Пусть сигнатура состоит из двуместного функционального символа f. Определим интерпретации I_1 и I_2 следующим образом. Носитель интерпретации I_1 — множество четных целых чисел; $\overline{f}(x, y) = x + y$. Носитель интерпретации I_2 — множество целых чисел, делящихся без остатка на 3; $\widetilde{f}(x, y) = x + y$. Функция $\varphi(x) = \frac{3}{2}x$ — изоморфизм из I_1 в I_2.

Пример 2. Пусть сигнатура состоит из константы a, двуместного функционального символа f и двуместного предикатного символа P. Носитель интерпретации I_1 — множество натуральных чисел; $\overline{a} = 0$; $\overline{f}(x, y) = x + y$; $\overline{P}(x, y) = \text{И} \Leftrightarrow x < y$. Носитель интерпретации I_2 — множество всех натуральных чисел вида 2^n, где $n \in \mathbb{N}$; $\widetilde{a} = 1$; $\widetilde{f}(x, y) = x \cdot y$; $\widetilde{P}(x, y) = \text{И} \Leftrightarrow x < y$. Функция $\varphi(x) = 2^x$ — изоморфизм из I_1 в I_2, так как $2^{x+y} = 2^x \cdot 2^y$, $2^0 = 1$ и $x < y \Leftrightarrow 2^x < 2^y$.

Теорема 10. *Для любой интерпретации I выполнено $I \simeq I$. Если $I_1 \simeq I_2$, то $I_2 \simeq I_1$. Если $I_1 \simeq I_2$ и $I_2 \simeq I_3$, то $I_1 \simeq I_3$.*

Доказательство. Тождественная функция является изоморфизмом из I в I. Пусть функция φ_1 является изоморфизмом из I_1 в I_2. Тогда φ_1^{-1} является изоморфизмом из I_2 в I_1. Пусть φ_2 — изоморфизм из I_2 в I_3. Тогда $\varphi_1 \circ \varphi_2$ — изоморфизм из I_1 в I_3. Теорема 10 доказана.

Пример 2 (продолжение). Функция $\log_2 x$ является изоморфизмом из I_2 в I_1. Действительно, $\log_2 1 = 0$, $\log_2$ сохраняет f, так как $\log_2(x \cdot y) = \log_2 x + \log_2 y$, и сохраняет P, так как $x < y \Leftrightarrow$ $\Leftrightarrow \log_2 x < \log_2 y$.

Говорят, что интерпретации I_1 и I_2 одной и той же сигнатуры Ω *элементарно эквивалентны*, если для любой замкнутой формулы $\mathcal{A}$ сигнатуры Ω выполнено $I_1 \models \mathcal{A} \Leftrightarrow I_2 \models \mathcal{A}$. Элементарную эквивалентность I_1 и I_2 будем обозначать $I_1 \cong I_2$. Очевидно, что интерпретации I_1 и I_2 не являются элементарно эквивалентными тогда

и только тогда, когда найдется замкнутая формула $\mathcal{A}$, для которой $I_1 \models \mathcal{A}$, $I_2 \models \neg\mathcal{A}$.

Теорема 11. *Если интерпретации I_1 и I_2 сигнатуры Ω изоморфны, то они элементарно эквивалентны. Более того, если φ — изоморфизм из I_1 в I_2, а $\mathcal{A}(x_1, \ldots, x_n)$ — формула со свободными переменными $x_1, \ldots, x_n$ и $a_1, \ldots, a_n$ — произвольные элементы носителя I_1, то $I_1 \models \mathcal{A}(\underline{a}_1, \ldots, \underline{a}_n) \Leftrightarrow I_2 \models \mathcal{A}(\underline{\varphi a}_1, \ldots, \underline{\varphi a}_n)$.*

Доказательство. Пусть M_1 и M_2 — соответственно носители интерпретаций I_1 и I_2, и $\varphi : M_1 \to M_2$ — изоморфизм из I_1 в I_2. Обозначим через Ω^1 и Ω^2 сигнатуры, полученные из сигнатуры Ω добавлением имен элементов соответственно из M_1 и M_2.

Для любого терма t и формулы $\mathcal{A}$ сигнатуры Ω^1 обозначим через $\widehat{t}$ и $\widehat{\mathcal{A}}$ результаты замены в t и $\mathcal{A}$ для любого $m \in M_1$ его имени $\underline{m}$ на $\underline{\varphi m}$ — имя элемента $\varphi m \in M_2$. Значение терма t в интерпретации I_1 будем обозначать через $|t|^1$, а в I_2 — через $|t|^2$.

Лемма 1. *Для любого замкнутого терма t сигнатуры Ω^1 выполнено $\varphi|t|^1 = |\widehat{t}|^2$.*

Доказательство. Индукция по построению t.

1) Пусть $t \rightleftharpoons c$, где c — константа из Ω. Тогда $\widehat{t} \rightleftharpoons c$, $|t|^1 = \overline{c}$, $|\widehat{t}|^2 = \widetilde{c}$, $\varphi\overline{c} = \widetilde{c}$, так как φ сохраняет константы из Ω.

2) Пусть $t \rightleftharpoons \underline{m}$, где $m \in M_1$. Тогда $\widehat{t} \rightleftharpoons \underline{\varphi m}$, $|t|^1 = m$, $|\widehat{t}|^2 = \varphi m$, т. е. $\varphi|t|^1 = |\widehat{t}|^2$.

3) Пусть $t \rightleftharpoons f(t_1, \ldots, t_n)$, причем $\varphi|t_i|^1 = |\widehat{t_i}|^2$ $(i = 1, \ldots, n)$. Тогда $\widehat{t} \rightleftharpoons f(\widehat{t_1}, \ldots, \widehat{t_n})$, $|t|^1 = \overline{f}(|t_1|^1, \ldots, |t_n|^1)$. Так как φ сохраняет f, то

$$\varphi|t|^1 = \varphi\overline{f}(|t_1|^1, \ldots, |t_n|^1) = \widetilde{f}(\varphi|t_1|^1, \ldots, \varphi|t_n|^1) = \\ = \widetilde{f}(|\widehat{t_1}|^2, \ldots, |\widehat{t_n}|^2) = |\widehat{t}|^2.$$

Лемма доказана.

Лемма 2. *Для любой замкнутой формулы $\mathcal{A}$ сигнатуры Ω^1 выполнено $I_1 \models \mathcal{A} \Leftrightarrow I_2 \models \widehat{\mathcal{A}}$.*

Доказательство. В силу теоремы 6 достаточно доказать лемму для формул $\mathcal{A}$, не содержащих &, $\supset$, $\equiv$, $\forall$. Применим индукцию по количеству символов $\exists, \neg, \vee$ в формуле $\mathcal{A}$.

а) Пусть $\mathcal{A} \rightleftharpoons P(t_1, \ldots, t_n)$. Тогда $\widehat{\mathcal{A}} \rightleftharpoons P(\widehat{t_1}, \ldots, \widehat{t_n})$. $I_1 \models \mathcal{A} \Leftrightarrow$ $\Leftrightarrow \overline{P}(|t_1|^1, \ldots, |t_n|^1) =$И. Так как φ сохраняет P, то $\overline{P}(|t_1^1|, \ldots, |t_n|^1) =$

$=\widetilde{P}(\varphi|t_1|^1, \dots, \varphi|t_n|^1)$. По лемме 1 $\varphi|t_i|^1 = |\widehat{t_i}|^2$. Поэтому $I_1 \models \mathcal{A} \Leftrightarrow$ $\Leftrightarrow \widetilde{P}(|\widehat{t_1}|^2, \dots, |\widehat{t_n}|^2) = \text{И} \Leftrightarrow I_2 \models \mathcal{A}$.

б) Пусть $\mathcal{A} \coloneqq t_1 = t_2$. Тогда $\widehat{\mathcal{A}} \coloneqq \widehat{t_1} = \widehat{t_2}$. $I_1 \models \mathcal{A} \Leftrightarrow |t_1|^1 = |t_2|^1 \Leftrightarrow$ $\Leftrightarrow \varphi|t_1|^1 = \varphi|t_2|^1 \Leftrightarrow |\widehat{t_1}|^2 = |\widehat{t_2}|^2 \Leftrightarrow I_2 \models \widehat{t_1} = \widehat{t_2} \Leftrightarrow I_2 \models \widehat{\mathcal{A}}$.

в) Пусть $\mathcal{A} \coloneqq \neg\mathcal{B}$, причем $I_1 \models \mathcal{B} \Leftrightarrow I_2 \models \widehat{\mathcal{B}}$. Тогда $\widehat{\mathcal{A}} \coloneqq \neg\widehat{\mathcal{B}}$. $I_1 \models \mathcal{A} \Leftrightarrow I_1 \not\models \mathcal{B} \Leftrightarrow I_2 \not\models \widehat{\mathcal{B}} \Leftrightarrow I_2 \models \widehat{\mathcal{A}}$.

г) Пусть $\mathcal{A} \coloneqq (\mathcal{B} \vee \mathcal{C})$, причем $I_1 \models \mathcal{B} \Leftrightarrow I_2 \models \widehat{\mathcal{B}}$ и $I_1 \models \mathcal{C} \Leftrightarrow$ $\Leftrightarrow I_2 \models \widehat{\mathcal{C}}$. Тогда $\widehat{\mathcal{A}} \coloneqq (\widehat{\mathcal{B}} \vee \widehat{\mathcal{C}})$. $I_1 \models \mathcal{A} \Leftrightarrow (I_1 \models \mathcal{B}$ или $I_1 \models \mathcal{C}) \Leftrightarrow$ $\Leftrightarrow (I_2 \models \widehat{\mathcal{B}}$ или $I_2 \models \widehat{\mathcal{C}}) \Leftrightarrow I_2 \models (\widehat{\mathcal{B}} \vee \widehat{\mathcal{C}}) \Leftrightarrow I_2 \models \widehat{\mathcal{A}}$.

д) Пусть $\mathcal{A} \coloneqq \exists x\ \mathcal{B}(x)$, причем для любой замкнутой формулы вида $\mathcal{B}(t)$ имеет место $I_1 \models \mathcal{B}(t) \Leftrightarrow I_2 \models \widehat{\mathcal{B}(t)}$. Тогда $\widehat{\mathcal{A}} \coloneqq \exists x\ \widehat{\mathcal{B}}(x)$. $I_1 \models \mathcal{A} \Leftrightarrow I_1 \models \mathcal{B}(\underline{m})$ для некоторого $m \in M_1 \Leftrightarrow I_2 \models \widehat{\mathcal{B}(m)}$ для некоторого $m \in M_1$. Легко видеть, что $\widehat{\mathcal{B}(m)} \coloneqq \widehat{\mathcal{B}}(\underline{\varphi m})$. Поэтому $I_1 \models \mathcal{B}(\underline{m}) \Leftrightarrow I_2 \models \widehat{\mathcal{B}}(\underline{\varphi m})$. Так как φ — биекция, то φm пробегает все множество M_2, когда m пробегает M_1. Поэтому мы имеем $I_1 \models \mathcal{A} \Leftrightarrow I_2 \models \widehat{\mathcal{B}}(\underline{\varphi m})$ для некоторого $m \in M_1 \Leftrightarrow I_2 \models \widehat{\mathcal{B}}(\underline{n})$ для некоторого $n \in M_2 \Leftrightarrow I_2 \models \exists x\ \widehat{\mathcal{B}}(x) \Leftrightarrow I_2 \models \widehat{\mathcal{A}}$.

Лемма доказана.

Применим лемму 2 к произвольной замкнутой формуле $\mathcal{A}$ сигнатуры Ω. Так как в этом случае $\widehat{\mathcal{A}}$ совпадает с $\mathcal{A}$, мы имеем $I_1 \models \mathcal{A} \Leftrightarrow I_2 \models \mathcal{A}$. В силу произвольности выбора $\mathcal{A}$ это означает, что $I_1 \cong I_2$.

Пусть теперь $\mathcal{A}(x_1, \dots, x_n)$ — произвольная формула со свободными переменными $x_1, \dots, x_n$, и $a_1, \dots, a_n$ — произвольные элементы из M_1. Положим $\mathcal{B} \coloneqq \mathcal{A}(a_1, \dots, a_n)$. Тогда $\widehat{\mathcal{B}} \coloneqq \mathcal{A}(\underline{\varphi a_1}, \dots, \underline{\varphi a_n})$. По лемме 2 имеем $I_1 \models \mathcal{B} \Leftrightarrow I_2 \models \widehat{\mathcal{B}}$, т. е. $I_1 \models \mathcal{A}(\underline{a_1}, \dots, \underline{a_n}) \Leftrightarrow$ $\Leftrightarrow I_2 \models \mathcal{A}(\underline{\varphi a_1}, \dots, \underline{\varphi a_n})$, что составляет вторую часть утверждения теоремы. Теорема 11 доказана.

Переформулировав теорему 11, получим: не элементарно эквивалентные интерпретации неизоморфны. В таком виде теорема 11 обычно используется при доказательстве неизоморфности.

Пример 3. Обозначим через $(\mathbb{N}, <)$ упорядоченное множество натуральных чисел, а через $(\mathbb{Z}, <)$ — упорядоченное множество целых чисел. Говоря формально, $(\mathbb{N}, <)$ и $(\mathbb{Z}, <)$ — интерпретации сигнатуры $\{<\}$ (т. е. сигнатуры $\Omega = \langle \mathrm{Cnst}, \mathrm{Fn}, \mathrm{Pr} \rangle$, где $\mathrm{Cnst} = \mathrm{Fn} = \varnothing$, $\mathrm{Pr} = \{<\}$) с носителями соответственно $\mathbb{N}$ и $\mathbb{Z}$ и стандартной интерпретацией символа $<$, а именно, $\overline{<}(x, y) = \text{И} \Leftrightarrow x < y$. Изоморфны

ли $(\mathbb{N},<)$ и $(\mathbb{Z},<)$? Разумеется, нет. Ведь в $(\mathbb{N},<)$ есть наименьший элемент, а в $(\mathbb{Z},<)$ его нет. Иными словами,

$$(\mathbb{N},<) \models \exists x\ \forall y\ (x<y \vee x=y);$$
$$(\mathbb{Z},<) \models \neg\exists x\ \forall y\ (x<y \vee x=y).$$

Таким образом, мы доказали, что $(\mathbb{N},<)$ и $(\mathbb{Z},<)$ не элементарно эквивалентны, а из этого уже вывели их неизоморфность.

Существуют ли неизоморфные интерпретации, неизоморфность которых нельзя доказать с помощью теоремы 11? Иными словами, существуют ли неизоморфные элементарно эквивалентные интерпретации? Оказывается, существуют. Без доказательства рассмотрим следующий пример.

Пример 4. Обозначим через $(\mathbb{Q},<)$ и $(\mathbb{R},<)$ упорядоченные множества соответственно рациональных и действительных чисел. Рассмотрим их как интерпретации сигнатуры $\{<\}$. Тогда $(\mathbb{Q},<) \not\simeq$ $\not\simeq (\mathbb{R},<)$, поскольку $\mathbb{Q}$ и $\mathbb{R}$ неравномощны. С помощью так называемой *элиминации кванторов* можно доказать, что $(\mathbb{Q},<) \cong (\mathbb{R},<)$.

Упражнения.

1. Доказать, что интерпретации $(\mathbb{R},+,<)$ и $(\mathbb{R}^+,\cdot,<)$, где $\mathbb{R}^+$ — множество положительных действительных чисел, изоморфны.

2. Доказать, что следующие интерпретации не являются элементарно эквивалентными:

а) $(\mathbb{Q},<)$ и $(\mathbb{Z},<)$;

б) $(\mathbb{Z},+)$ и $(\mathbb{Q},+)$;

в) $(\mathbb{Q},+,\cdot)$ и $(\mathbb{R},+,\cdot)$;

г) $(\mathbb{R},+,<)$ и $(\mathbb{C},+,\cdot)$;

д) $(\mathbb{N},+)$ и $(\mathbb{Z},+)$.

3. Доказать, что $(\mathbb{R},+) \simeq (\mathbb{R}^2,+)$, где сложение пар действительных чисел производится покомпонентно.

§ 14. Выразимость. Доказательство невыразимости с помощью автоморфизмов

Пусть $\mathcal{A}(x_1,\ldots,x_n)$ — формула сигнатуры Ω со свободными переменными $x_1,\ldots,x_n$, I — интерпретация сигнатуры Ω с носителем M, а R есть n-местный предикат на M. Говорят, что формула $\mathcal{A}$ *выражает* предикат R в интерпретации I, если $R(a_1,\ldots,a_n) = \text{И} \Leftrightarrow$ $\Leftrightarrow I \models \mathcal{A}(\underline{a}_1,\ldots,\underline{a}_n)$ для всех $a_1,\ldots,a_n \in M$.

Предикат R назовем *выразимым в интерпретации* I, если существует формула, его выражающая.

Пример 1. Возьмем стандартную интерпретацию языка формальной арифметики $(\mathbb{N}, +, \cdot, S, 0)$. Формула $\exists y\ x = y + y$ выражает предикат «x четно». Формула $\exists z\ x + z = y$ выражает предикат $x \leqslant y$. Формулы $x + x = x$ и $x = 0$ выражают один и тот же предикат $x = 0$. Можно ли выразить в этой интерпретации двуместный предикат $y = 2^x$? Оказывается, можно, хотя догадаться, как это сделать, довольно трудно.

Пример 2. Возьмем интерпретацию $(\mathbb{Z}, <)$. Формула

$$x < y \,\&\, \neg\exists z\ (x < z \,\&\, z < y)$$

выражает предикат $y = x+1$. Можно ли в $(\mathbb{Z}, <)$ выразить предикат $z = x + y$? Чуть позже мы докажем, что нельзя. Этому примеру можно придать следующий смысл. Пусть некто знает, что такое целые числа и что такое $x < y$ для целых x и y, но не знает никаких других отношений и функций на $\mathbb{Z}$. Тогда на языке первого порядка ему можно объяснить, что такое $y = x+1$, но нельзя объяснить, что такое $z = x + y$.

Пусть в определении изоморфизма интерпретации I_1 и I_2 совпадают; изоморфизмы из I в I называются *автоморфизмами* интерпретации I.

Определение автоморфизма φ очевидно принимает такой вид:
1) $\varphi\overline{c} = \overline{c}$ для всех констант c;
2) $\varphi\overline{f}(a_1, \ldots, a_n) = \overline{f}(\varphi a_1, \ldots, \varphi a_n)$ для всех $f \in \mathrm{Fn}$;
3) $\overline{P}(a_1, \ldots, a_n) = \overline{P}(\varphi a_1, \ldots, \varphi a_n)$ для всех $P \in \mathrm{Pr}$.

Пример 3. Для всех $k \in \mathbb{Z}$ отображение $\varphi_k(x) = x + k$ является автоморфизмом интерпретации $(\mathbb{Z}, <)$. Действительно, φ_k — биекция, и φ_k сохраняет $<$, так как $x < y \Leftrightarrow x + k < y + k$. В качестве упражнения предлагается доказать, что других автоморфизмов эта интерпретация не имеет. Например, отображение $\varphi(x) = 2x$ хоть и сохраняет $<$, но автоморфизмом не является, так как оно не биективно.

Теорема 12. *Множество всех автоморфизмов фиксированной интерпретации I образует группу относительно операции композиции.*

Эта теорема доказывается аналогично теореме 10.

Пусть R есть n-местный предикат на некотором множестве M, а φ — функция из M в M. Будем говорить, что φ *сохраняет* R, если для всех $a_1, \ldots, a_n \in M$ выполнено $R(a_1, \ldots, a_n) = R(\varphi a_1, \ldots, \varphi a_n)$.

Пример 3 (продолжение). Все автоморфизмы интерпретации $(\mathbb{Z}, <)$ сохраняют двуместный предикат $|x - y| = 2$. Действительно, любой автоморфизм $(\mathbb{Z}, <)$ имеет вид $\varphi_k(x) = x + k$, и $|x - y| = 2 \Leftrightarrow$ $\Leftrightarrow |(x + k) - (y + k)| = 2$.

Теорема 13. *Пусть φ — автоморфизм интерпретации I. Тогда φ сохраняет все выразимые в I предикаты.*

Доказательство. Пусть предикат $R(x_1, \ldots, x_n)$ выразим в I. Тогда для некоторой формулы $\mathcal{A}(x_1, \ldots, x_n)$ выполнено

$$R(a_1, \ldots, a_n) = \text{И} \Leftrightarrow I \models \mathcal{A}(\underline{a}_1, \ldots, \underline{a}_n).$$

По теореме 11 для всех $a_1, \ldots, a_n$ из носителя I выполнено

$$I \models \mathcal{A}(\underline{a}_1, \ldots, \underline{a}_n) \Leftrightarrow I \models \mathcal{A}(\underline{\varphi a_1}, \ldots, \underline{\varphi a_n}).$$

Из этих двух утверждений получаем

$$R(a_1, \ldots, a_n) = \text{И} \Leftrightarrow R(\varphi a_1, \ldots, \varphi a_n) = \text{И},$$

что и требовалось. Теорема 13 доказана.

Теорема 14. *Предикат $z = x + y$ невырази́м в интерпретации $(\mathbb{Z}, <)$.*

Доказательство. Возьмем автоморфизм $\varphi(x) = x + 1$ интерпретации $(\mathbb{Z}, <)$. Функция φ не сохраняет предикат $z = x + y$, так как $0 = 0 + 0$, но $\varphi(0) \neq \varphi(0) + \varphi(0)$, ведь $\varphi(0) = 1$. Теперь воспользуемся теоремой 13. Теорема 14 доказана.

Пример 4. Можно ли, используя только понятие «точки x, y, z лежат на одной прямой», на языке первого порядка объяснить, что такое перпендикулярность прямых? Сформулируем точнее вопрос. Пусть $(\mathbb{R}^2, T)$ обозначает интерпретацию сигнатуры с одним трехместным предикатным символом T, носитель которой — множество точек плоскости, а $\overline{T}(x, y, z) = \text{И}$ тогда и только тогда, когда точки x, y, z лежат на одной прямой. Вырази́м ли в $(\mathbb{R}^2, T)$ четырехместный предикат $R(x, y, z, u)$, определенный так: $R(x, y, z, u) = \text{И}$ тогда и только тогда, когда $x \neq y$, $z \neq u$ и прямая, проходящая через x и y, перпендикулярна прямой, проходящей через z и u? Ответ: не вырази́м, так как любое аффинное преобразование является автоморфизмом $(\mathbb{R}^2, T)$, а среди них есть преобразования, не сохраняющие углы.

Упражнения.

1. Доказать, что группа автоморфизмов интерпретации $(\mathbb{Z}, <)$ изоморфна группе целых чисел по сложению.

2. Какова группа автоморфизмов интерпретации $(\mathbb{Q}, +)$?

3. Доказать выразимость или невыразимость данного отношения в данной интерпретации:

а) $x < y$ в $(\mathbb{Z}, +)$;

б) $z = 0$ в $(\mathbb{Z}, x = y + 1)$;

в) $x = y + 1$ в $(\mathbb{Z}, |x - y| = 1)$;

г) $x = y + 1$ в $(\mathbb{Z}, x = y + 2)$;

д) $y = x + 17$ в $(\mathbb{N}, y = x + 1)$;

е) $y = x + 1$ в $(\mathbb{N}, <)$;

ж) $|x - y| = 17$ в $(\mathbb{R}, |x{=}y|{=}1)$;

з) $x = 1$ в $(\mathbb{N}, x \vdots y)$;

и) $|x - y| = \frac{1}{2}$ в $(\mathbb{C}, |x{-}y|{=}1)$;

к) $x = 17$ в $(\mathbb{N}, y = x + 1)$;

л) $x = 17$ в $(\mathbb{N}, y \vdots x)$;

м) «x — простое число» в $(\mathbb{N}, x \vdots y)$;

н) $z = x \cdot y$ в $(\mathbb{R}, +, y = x^2)$;

о)* $z = x \cdot y$ в $(\mathbb{N}, +,$ «x — полный квадрат»$)$;

п) $x \equiv 0 \pmod 3$ в $(\mathbb{Z}, +)$;

р) $x \equiv 1 \pmod 3$ в $(\mathbb{Z}, +)$.

ГЛАВА 3

ЭЛЕМЕНТЫ ТЕОРИИ ДОКАЗАТЕЛЬСТВ

§ 1. Аксиоматический метод

Аксиоматический метод построения научной теории заключается в том, что некоторые исходные положения, называемые *аксиомами* или *постулатами*, принимаются «без доказательства», а все утверждения этой теории выводятся из них путем рассуждений.

Аксиоматический метод в математике впервые был использован Евклидом в III веке до н. э. в его книге «Начала» при изложении основ элементарной геометрии, теории чисел, алгебры и других разделов античной математики. «Начала» Евклида составлены по определенной схеме, сложившейся еще до Евклида в древнегреческой науке: сначала приводятся определения и постулаты, а затем формулировки теорем и их доказательства.

Некоторые определения в «Началах» Евклида — просто описания исходных понятий. Например: «Точка есть то, что не имеет частей», «Линия же — длина без ширины», «Прямая линия есть та, которая равно расположена по отношению к точкам на ней». Ясно, что такие «определения» вряд ли могут быть использованы в математических доказательствах. Однако наряду с ними имеются определения, являющиеся таковыми и в современном смысле: они «называют» понятия. Например: «Параллельные суть прямые, которые, находясь в одной плоскости и будучи неограниченно продолжены в обе стороны, ни с той, ни с другой стороны между собой не встречаются».

Вслед за определениями идут постулаты, в которых утверждается возможность выполнения элементарных построений:

I. Требуется, чтобы от каждой точки ко всякой другой точке можно было провести прямую линию.

II. И чтобы каждую ограниченную прямую можно было непрерывно продолжить по прямой.

III. И чтобы из всякого центра и всяким радиусом можно было описать круг.

IV. И чтобы все прямые углы были равны между собой.

V. И чтобы всякий раз, когда прямая, падающая на две прямые, образует с ними внутренние односторонние углы, сумма которых меньше двух прямых, то эти прямые пересекаются с той стороны, где эта сумма меньше двух прямых.

За постулатами в «Началах» Евклида приводятся аксиомы — предложения о свойствах отношений равенства и неравенства. Вот примеры аксиом: «Равные порознь третьему равны между собой», «И если к равным прибавить равные, то получим равные», «И целое больше части».

На основе определений, постулатов и аксиом путем доказательства выводятся новые геометрические утверждения — теоремы.

Поскольку предполагалось, что геометрия есть описание реального физического пространства, вполне естественно, что Евклид полагал значение таких понятий, как «точка», «прямая», достаточно ясным, а относящиеся к ним постулаты и аксиомы считал «самоочевидными истинами».

В дальнейшем совершенствование аксиоматического изложения геометрии шло в основном по пути выявления утверждений, которые использовались Евклидом в доказательствах, но не были сформулированы им явно в виде аксиом. Полностью эта работа была завершена лишь в XIX веке Пашем и Гильбертом.

Вместе с тем, много усилий было потрачено на попытки исключить из числа основных допущений V постулат Евклида, который казался слишком сложным, чтобы его можно было причислить к “самоочевидным истинам”. Хотя все попытки доказать V постулат на основе отдельных аксиом оказались неудачными, они все же привели к некоторым положительным результатам. А именно, благодаря им был обнаружен ряд геометрических утверждений, эквивалентных V постулату, в частности, следующее: «Через каждую точку, не лежащую на прямой l, проходит в точности одна прямая, параллельная l».

К началу XIX века начало возникать подозрение о недоказуемости V постулата Евклида. Это подозрение перешло почти в полную уверенность, когда в 1826 году Лобачевский построил геометрическую теорию, основанную на системе постулатов, в которой V постулат Евклида заменен утверждением, несовместимым с ним: «Если на плоскости точка A не лежит на прямой l, то существует более чем одна прямая, проходящая через A и параллельная l». Хотя «истинность» такой аксиомы кажется сомнительной, при выводе следствий из нее Лобачевский не встретил каких-либо противоречий. Это, однако, не означало, что противоречия здесь вообще невозможны.

Следующим событием на пути укрепления позиций неевклидовой геометрии явилось построение различных моделей геометрии Лобачевского средствами геометрии Евклида. Типичным примером такого рода моделей может служить модель, предложенная Ф. Клейном в 1871 г. В этой модели основные геометрические понятия: плоскость, точка и прямая — интерпретируются соответственно как внутренность какого-нибудь круга в евклидовой плоскости, точка внутри этого круга и хорда этого круга, рассматриваемая без своих концов. В такой интерпретации оказываются истинными все аксиомы геометрии Лобачевского; правда, при этом расстояния и углы измеряются не так, как на обычной евклидовой плоскости, а по правилам, разработанным для проективной геометрии. Подробное описание интерпретации Клейна и других моделей геометрии Лобачевского можно найти в учебных пособиях по высшей геометрии*). Наличие таких моделей показывает, что геометрия Лобачевского столь же непротиворечива, как и геометрия Евклида.

Построение моделей геометрии Лобачевского имело принципиальное значение для развития аксиоматического метода, поскольку оно привело к осознанию возможности рассматривать аксиоматическую теорию чисто формально, т. е. не предполагая заранее какое-либо определенное значение основных понятий. Более того, мы вольны выбирать значения этих понятий каким угодно образом, лишь бы при этом оказывались истинными данные аксиомы.

В XIX в. аксиоматический метод получил широкое распространение в математике. Дж. Пеано (1891 г.) предложил аксиоматику для натурального ряда. Были построены аксиоматические теории для действительных чисел. Наконец, как мы уже говорили в главе 1, была выработана система аксиом для теории множеств. Особенно широкое распространение формальные аксиоматики получили в современной алгебре, где система аксиом по существу выступает в роли определения той или иной алгебраической структуры.

Пример 1. *Теория групп.* В алгебре группа определяется как непустое множество G, на котором задана бинарная операция $\cdot$, удовлетворяющая следующим аксиомам:

1) операция $\cdot$ ассоциативна;

2) во множестве G существует единичный элемент, т. е. такой элемент e, что для любого $a \in G$ выполняются равенства $a \cdot e = a$ и $e \cdot a = a$;

*) См., например, *Ефимов Н.В.* Высшая геометрия. — М.: ФИЗМАТЛИТ, 2003.

3) для любого $a \in G$ имеется обратный элемент, т. е. такой элемент $a' \in G$, что $a \cdot a' = e$ и $a' \cdot a = e$.

Очевидно, что эти аксиомы могут быть записаны на языке первого порядка, сигнатура которого содержит константу e и двуместный функциональный символ $\cdot$, в виде следующих формул:

$G1$. $\forall x\ \forall y\ \forall z\ (x \cdot y) \cdot z = x \cdot (y \cdot z)$;

$G2$. $\forall x\ (x \cdot e = x\ \&\ e \cdot x = x)$;

$G3$. $\forall x\ \exists y\ (x \cdot y = e\ \&\ y \cdot x = e)$.

Систему аксиом $G1$–$G3$ назовем системой аксиом для теории групп и обозначим ее G. Всякая интерпретация, в которой истинны аксиомы теории групп, является (или называется) *группой*.

Пример 2. *Теория линейно упорядоченных множеств.* Аксиомы линейно упорядоченного множества записываются в виде формул языка первого порядка, сигнатура которого содержит только двуместный предикатный символ $<$. Вот эти аксиомы:

$LO1$. $\forall x\ \neg x < x$;

$LO2$. $\forall x\ \forall y\ \forall z\ (x < y\ \&\ y < z \supset x < z)$;

$LO3$. $\forall x\ \forall y\ (x < y \vee x = y \vee y < x)$.

Формулы $LO1$ и $LO2$ называются аксиомами предпорядка, а формула $LO3$ — аксиомой линейной упорядоченности. Систему аксиом для теории линейно упорядоченных множеств обозначим LO. *Линейно упорядоченное множество* — это такая интерпретация рассматриваемого языка, в которой истинны аксиомы $LO1$–$LO3$.

Пример 3. *Теория полей.* Аксиомы поля записываются в виде формул языка первого порядка, сигнатура которого содержит константы 0 и 1, а также двуместные функциональные символы $+$ и $\cdot$. Вот аксиомы поля:

$F1$. $\forall x\ \forall y\ x + y = y + x$;

$F2$. $\forall x\ \forall y\ \forall z\ (x + y) + z = x + (y + z)$;

$F3$. $\forall x\ x + 0 = x$;

$F4$. $\forall x\ \exists y\ x + y = 0$;

$F5$. $\forall x\ \forall y\ x \cdot y = y \cdot x$;

$F6$. $\forall x\ \forall y\ \forall z\ (x \cdot y) \cdot z = x \cdot (y \cdot z)$;

$F7$. $\forall x\ x \cdot 1 = x$;

$F8$. $\forall x\ (\neg x = 0 \supset \exists y\ x \cdot y = 1)$;

$F9$. $\forall x\ \forall y\ \forall z\ (x + y) \cdot z = (x \cdot z) + (y \cdot z)$;

$F10$. $\neg 0 = 1$.

Систему аксиом $F1$–$F10$ обозначим F. *Поле* — это такая интерпретация, в которой истинны все формулы $F1$–$F10$.

§ 2. Логическое следование

Теперь рассмотрим вопрос: какие утверждения следует считать относящимися к данной аксиоматической теории? Например, можно ли считать фактом теории групп утверждение, выражаемое формулой $\forall x\ \forall y\ x \cdot y = y \cdot x$? Очевидно, нет, потому что существуют группы, в которых это утверждение неверно. (Группы, в которых это утверждение истинно, называются *абелевыми.*) Иными словами, можно сказать, что это утверждение не вытекает логически из аксиом. Это наблюдение помогает выразить понятие логического следования в виде точных определений.

При рассмотрении аксиоматических теорий в общем виде приходится считаться с тем, что любое множество замкнутых формул данного языка первого порядка может быть принято в качестве системы аксиом. Итак, пусть T — произвольное множество замкнутых формул сигнатуры Ω. *Моделью* множества T называется интерпретация I сигнатуры Ω, в которой истинны все формулы из T. Множество T называется *совместным*, если оно имеет хотя бы одну модель.

Таким образом, модели системы аксиом G — это в точности все группы, модели системы аксиом LO — все линейно упорядоченные множества, модели системы аксиом F — это все поля. Очевидно, что все эти системы аксиом совместны. А вот пример несовместного множества формул (доказательство предлагается в качестве упражнения):

$$\{\forall x\ \forall y\ x = y,\ \exists y\ \exists z\ (P(y)\ \&\ \neg P(z))\}.$$

Будем говорить, что замкнутая формула $\mathcal{A}$ сигнатуры Ω *логически следует* (*семантически следует* или просто *следует*) из T, и писать $T \models \mathcal{A}$, если $\mathcal{A}$ истинна во всех моделях множества T. В этом случае будем говорить также, что $\mathcal{A}$ является *логическим следствием* множества формул T.

Теорема 1. *Пусть T — некоторое множество замкнутых формул сигнатуры Ω, а $\mathcal{A}$ и $\mathcal{B}$ — замкнутые формулы сигнатуры Ω. Тогда*

а) $(T \models \mathcal{A}$ и $T \models \mathcal{B}) \Leftrightarrow T \models \mathcal{A}\ \&\ \mathcal{B}$;

б) $T \cup \{\mathcal{A}\} \models \mathcal{B} \Leftrightarrow T \models \mathcal{A} \supset \mathcal{B}$;

в) $T \models \mathcal{A} \Leftrightarrow$ множество $T \cup \{\neg\mathcal{A}\}$ несовместно.

Доказательство. Утверждение а) очевидно.

Докажем б). Пусть $T \cup \{\mathcal{A}\} \models \mathcal{B}$, и пусть I — произвольная модель множества T. Если $I \not\models \mathcal{A}$, то по определению истинности $I \models \mathcal{A} \supset \mathcal{B}$. Если же $I \models \mathcal{A}$, то I является моделью множества $T \cup \{\mathcal{A}\}$, и по условию $I \models \mathcal{B}$. Значит, и в этом случае $I \models \mathcal{A} \supset \mathcal{B}$. Таким образом, формула $\mathcal{A} \supset \mathcal{B}$ истинна в любой модели множества T, т. е. $T \models \mathcal{A} \supset \mathcal{B}$.

Обратно, если $T \models \mathcal{A} \supset \mathcal{B}$ и I — произвольная модель множества $T \cup \{\mathcal{A}\}$, то $I \models \mathcal{A} \supset \mathcal{B}$ и $I \models \mathcal{A}$. Отсюда немедленно следует, что $I \models \mathcal{B}$. Значит, $\mathcal{B}$ истинна в любой модели множества $T \cup \{\mathcal{A}\}$, т. е. $T \cup \{\mathcal{A}\} \models \mathcal{B}$.

Теперь докажем в). Пусть $T \models \mathcal{A}$. Допустим, что множество $T \cup \{\neg\mathcal{A}\}$ совместно, т. е. существует его модель I. Тогда $I \models \neg\mathcal{A}$ и I является также моделью для T. По условию в этом случае $I \models \mathcal{A}$. Значит, $I \models \mathcal{A}$ и $I \models \neg\mathcal{A}$, т. е. $I \not\models \mathcal{A}$. Полученное противоречие показывает, что множество $T \cup \{\neg\mathcal{A}\}$ на самом деле несовместно.

Пусть множество $T \cup \{\neg\mathcal{A}\}$ несовместно, т. е. не имеет модели, и пусть I — произвольная модель множества T. Тогда $I \models \mathcal{A}$, так как иначе $I \models \neg\mathcal{A}$ и I была бы моделью множества $T \cup \{\neg\mathcal{A}\}$. Значит, $\mathcal{A}$ истинна в любой модели множества T, т. е. $T \models \mathcal{A}$. Теорема доказана.

Множество T замкнутых формул сигнатуры Ω будем называть *семантически полным*, если T совместно и для любой замкнутой формулы $\mathcal{A}$ сигнатуры Ω выполнено $T \models \mathcal{A}$ или $T \models \neg\mathcal{A}$.

Пример 1. Пусть сигнатура не содержит никаких констант, функциональных и предикатных символов (пустая сигнатура). Рассмотрим следующее одноэлементное множество формул этой сигнатуры: $T = \{\forall x\ \forall y\ x = y\}$. Это множество семантически полно, поскольку оно имеет единственную, с точностью до изоморфизма, модель — одноэлементное множество, и любая замкнутая формула либо истинна, либо ложна в этой модели.

Теорема 2. *Совместное множество формул T семантически полно тогда и только тогда, когда любые две его модели элементарно эквивалентны.*

Доказательство. Пусть множество T семантически полно, и пусть I_1 и I_2 — две его модели. Допустим, что существует такая замкнутая формула $\mathcal{A}$, что $I_1 \models \mathcal{A}$ и $I_2 \not\models \mathcal{A}$. Тогда $T \not\models \mathcal{A}$, так как $I_2 \not\models \mathcal{A}$, и $T \not\models \neg\mathcal{A}$, так как $I_1 \not\models \neg\mathcal{A}$. Полученное противоречие определению семантической полноты показывает, что такой формулы $\mathcal{A}$ не существует, т. е. $I_1 \cong I_2$.

Обратно, пусть любые две модели множества T элементарно эквивалентны. Пусть $\mathcal{A}$ — произвольная замкнутая формула. По условию T совместно, т. е. имеет некоторую модель I_0. Очевидно, $I_0 \models \mathcal{A}$ или $I_0 \models \neg\mathcal{A}$. Пусть для определенности $I_0 \models \mathcal{A}$ и пусть I — произвольная модель множества T. Так как $I \cong I_0$, то $I \models \mathcal{A}$, т. е. $\mathcal{A}$ истинна в любой модели множества T, и $T \models \mathcal{A}$.

Аналогично доказывается, что если $I_0 \models \neg\mathcal{A}$, то $T \models \neg\mathcal{A}$. Теорема доказана.

Ни одна из систем аксиом G, LO, F не является семантически полной. Без доказательства приведем два нетривиальных примера семантически полных систем аксиом. Первая получается добавлением к LO аксиом

$$\begin{aligned}&\forall x\ \exists y\ x < y;\\ &\forall x\ \exists y\ y < x;\\ &\forall x\ \forall y\ (x < y \supset \exists z\ (x < z\ \&\ z < y)).\end{aligned}$$

Эта система аксиом задает понятие *плотного линейного порядка без первого и последнего элементов* и обозначается DLO.

Другой нетривиальный пример семантически полной системы аксиом — это система аксиом *алгебраически замкнутых полей характеристики ноль* $ACF0$, которая получается добавлением к F двух бесконечных множеств формул $\{\mathcal{A}_k \mid k \in \mathbb{N},\ k \geqslant 2\}$ и $\{\mathcal{B}_k \mid k \in \mathbb{N},\ k \geqslant 2\}$, где

$$\mathcal{A}_k \rightleftharpoons \neg(\underbrace{\ldots((1+1)+1)\ldots+1)+1}_{k\text{ единиц}} = 0,$$

$$\mathcal{B}_k \rightleftharpoons \forall y_0 \forall y_1 \ldots \forall y_k\ (\neg y_k = 0 \supset \exists z\ (y_k \cdot z^k + \ldots + y_1 \cdot z + y_0 = 0))$$

(здесь $z^n \rightleftharpoons \underbrace{(\ldots((z \cdot z) \cdot z) \cdot \ldots \cdot z) \cdot z}_{n\text{ раз}}$).

Итак, мы уточнили, что значит, что данное утверждение логически следует из данной системы аксиом. Как же практически можно искать логические следствия из аксиом? Ясно, что нет смысла действовать в полном соответствии с определением логического следования, т. е. перебирать все модели данной системы аксиом и убеждаться, что в них истинно данное утверждение, поскольку, во-первых, нам не всегда известны все модели, а, во-вторых, их может оказаться бесконечно много (как, например, групп). Все же иногда

(и даже очень часто) путем некоторого рассуждения удается доказать, что то или иное утверждение логически следует из аксиом. Тогда такое рассуждение мы называем доказательством, а полученное с его помощью следствие из аксиом — теоремой. Оказывается, что таким образом можно доказать любое утверждение, логически вытекающее из аксиом, записанных в виде формул языка первого порядка, а необходимые для этого методы доказательства можно полностью обозреть и систематизировать. Это делается с помощью так называемого *исчисления предикатов.*

Упражнения. 1. Доказать, что аксиомы теории групп логически следуют из множества формул

$$\{\forall x\ \forall y\ \forall z\ x \cdot (y \cdot z) = (x \cdot y) \cdot z,\ \forall x\ x \cdot e = x,\ \forall x\ \exists y\ x \cdot y = e\}$$

и не следуют из множества формул, полученного из этого заменой последней формулы на формулу $\forall x\ \exists y\ y \cdot x = e$.

2. Доказать, что формулы $\forall x\ \forall y\ (x \cdot y = 0 \supset x = 0 \vee y = 0)$ и $\forall x\ x \cdot 0 = 0$ логически следуют из аксиом поля, а формула

$$\forall x\ (x + x = 0 \supset x = 0)$$

не следует.

§ 3. Тавтологическое следствие

В § 10 главы 2 было введено понятие тавтологии как формулы языка первого порядка, которая получается из некоторой пропозициональной тавтологии подстановкой каких-либо формул языка первого порядка вместо пропозициональных переменных. Будем говорить, что формула $\mathcal{A}$ языка первого порядка является *тавтологическим следствием* формул $\mathcal{A}_1, \ldots, \mathcal{A}_n$ того же языка, если формула $\mathcal{A}_1 \& \ldots \& \mathcal{A}_n \supset \mathcal{A}$ есть тавтология.

Пример 1. Формула $P(z)$ является тавтологическим следствием формул $\exists y\ Q(y)$ и $\exists y\ Q(y) \supset P(z)$. Действительно, формула $\exists y\ Q(y) \& (\exists y\ Q(y) \supset P(z)) \supset P(z)$ есть тавтология: она получается подстановкой в пропозициональную тавтологию $P \& (P \supset Q) \supset Q$ формулы $\exists y\ Q(y)$ вместо пропозициональной переменной P и $P(z)$ вместо Q.

Теорема 3. *Тавтологическое следствие общезначимых формул общезначимо.*

Доказательство. Пусть $\mathcal{A}$ — тавтологическое следствие общезначимых формул $\mathcal{A}_1, \ldots, \mathcal{A}_n$. Пусть I — произвольная интерпретация, θ — произвольная оценка формулы $\mathcal{A}$. Произвольным образом расширим оценку θ, чтобы она стала оценкой формул $\mathcal{A}_1, \ldots, \mathcal{A}_n$, т. е. придадим какие-нибудь значения и тем переменным, которые входят свободно в эти формулы, но не получают значений при оценке θ. Полученную оценку обозначим θ'. Очевидно, что $\theta'\mathcal{A} \rightleftharpoons \theta\mathcal{A}$. По условию формула $\mathcal{A}_1 \mathbin{\&} \ldots \mathbin{\&} \mathcal{A}_n \supset \mathcal{A}$ — тавтология. По теореме 1 из главы 2 она общезначима. Значит, $I \models \theta'(\mathcal{A}_1 \mathbin{\&} \ldots \mathbin{\&} \mathcal{A}_n \supset \mathcal{A})$. Но

$$\theta'(\mathcal{A}_1 \mathbin{\&} \ldots \mathbin{\&} \mathcal{A}_n \supset \mathcal{A}) \rightleftharpoons (\theta'\mathcal{A}_1 \mathbin{\&} \ldots \mathbin{\&} \theta'\mathcal{A}_n \supset \theta'\mathcal{A}).$$

Так как формулы $\mathcal{A}_1, \ldots, \mathcal{A}_n$ общезначимы, то $I \models \theta'\mathcal{A}_1$, ..., $I \models \theta'\mathcal{A}_n$. Отсюда немедленно следует, что $I \models \theta'\mathcal{A}$, т. е. $I \models \theta\mathcal{A}$. Таким образом, формула $\mathcal{A}$ истинна в любой интерпретации при любой оценке, т. е. $\mathcal{A}$ общезначима. Теорема доказана.

§ 4. Исчисление предикатов

Фиксируем некоторую сигнатуру Ω. Аксиомами исчисления предикатов в сигнатуре Ω называются следующие формулы:

(a1) любая тавтология сигнатуры Ω;

(a2) $\mathcal{A}(t) \supset \exists x \mathcal{A}(x)$;

(a3) $\forall x\ \mathcal{A}(x) \supset \mathcal{A}(t)$;

(a4) $\forall x\ (\mathcal{A}(x) \supset \mathcal{B}) \supset (\exists x\ \mathcal{A}(x) \supset \mathcal{B})$;

(a5) $\forall x\ (\mathcal{B} \supset \mathcal{A}(x)) \supset (\mathcal{B} \supset \forall x\ \mathcal{A}(x))$;

(a6) $t_1 = t_1$;

(a7) $t_1 = t_2 \supset t_2 = t_1$;

(a8) $t_1 = t_2 \mathbin{\&} t_2 = t_3 \supset t_1 = t_3$;

(a9) $t_1 = s_1 \mathbin{\&} \ldots \mathbin{\&} t_n = s_n \supset f(t_1, \ldots, t_n) = f(s_1, \ldots, s_n)$;

(a10) $t_1 = s_1 \mathbin{\&} \ldots \mathbin{\&} t_n = s_n \supset (P(t_1, \ldots, t_n) \equiv P(s_1, \ldots, s_n))$.

Здесь $\mathcal{A}(x)$ — любая формула сигнатуры Ω, x — любая переменная, терм t свободен для x в $\mathcal{A}(x)$; $\mathcal{B}$ — любая формула сигнатуры Ω, не содержащая свободных вхождений x; $t_1, \ldots, t_n, s_1, \ldots, s_n$ — любые термы, f — любой n-местный функциональный символ из Ω, P — любой n-местный предикатный символ из Ω.

Множество аксиом в каждой из групп бесконечно: фиксируя $\mathcal{A}(x)$, $\mathcal{B}, t_1, \dots, t_n, s_1, \dots, s_n, f, P$, можно получить любую конкретную аксиому. Аксиомы (а6)–(а10) называются *аксиомами равенства.*

Пример 1. Формула $0+0=y \supset \exists x\; x+x=y$ является аксиомой из группы (а2), или просто аксиомой (а2). Здесь $\mathcal{A}(x) \rightleftharpoons x+x=y,\ t \rightleftharpoons 0$. Формула $\forall x\; x\cdot y = y\cdot x \supset (z_1+z_2)\cdot y = y\cdot(z_1+z_2)$ является аксиомой (а3). Здесь $\mathcal{A}(x) \rightleftharpoons x\cdot y = y\cdot x,\ t \rightleftharpoons z_1+z_2$.

Пример 2. Вот примеры аксиом (а9), (а10):

$$x=y\ \&\ z=u \supset x+z=y+u;$$

$$x=y\ \&\ z=u \supset (x<z \equiv y<u).$$

Любое множество фигур вида $\dfrac{\mathcal{A}_1, \dots, \mathcal{A}_n}{\mathcal{A}}$, где $\mathcal{A}_1, \dots, \mathcal{A}_n, \mathcal{A}$ — формулы, называется *правилом вывода.* Будем говорить, что формула $\mathcal{A}$ получена из формул $\mathcal{A}_1, \dots, \mathcal{A}_n$ по правилу Π, если

$$\frac{\mathcal{A}_1, \dots, \mathcal{A}_n}{\mathcal{A}} \in \Pi.$$

В исчислении предикатов два правила вывода: *правило тавтологического следствия*

$$(Taut) = \left\{ \frac{\mathcal{A}_1, \dots, \mathcal{A}_n}{\mathcal{A}} \middle| \mathcal{A} \text{ — тавтологическое следствие } \mathcal{A}_1, \dots, \mathcal{A}_n \right\}$$

и *правило обобщения*

$$(Gen) = \left\{ \frac{\mathcal{A}}{\forall x \mathcal{A}} \middle| \begin{array}{l} \mathcal{A} \text{ — любая формула сигнатуры } \Omega, \\ x \text{ — любая переменная} \end{array} \right\}.$$

Вот некоторые часто применяющиеся виды фигур, содержащиеся в правиле $(Taut)$:

1) $\dfrac{\mathcal{A}, \mathcal{A} \supset \mathcal{B}}{\mathcal{B}}$, где $\mathcal{A}$ и $\mathcal{B}$ — произвольные формулы сигнатуры Ω. Совокупность таких фигур называют *правилом заключения* или *modus ponens*, сокращенно (MP).

2) $\dfrac{\mathcal{A} \supset \mathcal{B}, \mathcal{B} \supset \mathcal{C}}{\mathcal{A} \supset \mathcal{C}}$, где $\mathcal{A}, \mathcal{B}, \mathcal{C}$ — произвольные формулы сигнатуры Ω. Совокупность таких фигур называется *правилом силлогизма.*

3) $\dfrac{\mathcal{A} \supset \mathcal{B}}{\neg\mathcal{B} \supset \neg\mathcal{A}}$, $\dfrac{\neg\mathcal{A} \supset \neg\mathcal{B}}{\mathcal{B} \supset \mathcal{A}}$, $\dfrac{\mathcal{A} \supset \neg\mathcal{B}}{\mathcal{B} \supset \neg\mathcal{A}}$, $\dfrac{\neg\mathcal{A} \supset \mathcal{B}}{\neg\mathcal{B} \supset \mathcal{A}}$, где $\mathcal{A}$, $\mathcal{B}$ — произвольные формулы сигнатуры Ω. Совокупность таких фигур называют *правилом контрапозиции.*

Последовательность формул $\mathcal{B}_1, \dots, \mathcal{B}_n$ называется *выводом*, если для всех $i \le n$ формула $\mathcal{B}_i$ либо есть аксиома исчисления предикатов, либо получена из предыдущих формул этой последовательности по одному из правил вывода $(Taut)$ или (Gen). Формула $\mathcal{B}$ *выводима*, если существует вывод $\mathcal{B}_1, \dots, \mathcal{B}_n$ такой, что $\mathcal{B}_n \rightleftharpoons \mathcal{B}$.

Пример 3. Установим выводимость формулы

$$\exists x\ \forall y\ P(x,y) \supset \forall y\ \exists x\ P(x,y).$$

1. $\forall y\ P(x,y) \supset P(x,y)$ (аксиома $(a3)$);
2. $P(x,y) \supset \exists x\ P(x,y)$ (аксиома $(a2)$);
3. $\forall y\ P(x,y) \supset \exists x\ P(x,y)$ (получена из 1. и 2. по правилу силлогизма);
4. $\forall x\ (\forall y\ P(x,y) \supset \exists x\ P(x,y))$ (получена из 3. по правилу (Gen));
5. $\forall x\ (\forall y\ P(x,y) \supset \exists x\ P(x,y)) \supset (\exists x\ \forall y\ P(x,y) \supset \exists x\ P(x,y))$ (аксиома (a4));
6. $\exists x\ \forall y\ P(x,y) \supset \exists x\ P(x,y)$ (получена из 4. и 5. по (MP));
7. $\forall y\ (\exists x\ \forall y\ P(x,y) \supset \exists x\ P(x,y))$ (получена из 6. по (Gen));
8. $\forall y\ (\exists x\ \forall y\ P(x,y) \supset \exists x\ P(x,y)) \supset (\exists x\ \forall y\ P(x,y) \supset \forall y\ \exists x\ P(x,y))$ (аксиома (a5));
9. $\exists x\ \forall y\ P(x,\ y) \supset \forall y\ \exists x\ P(x,y)$ (получена из 7. и 8. по (MP)).

Теорема 4 (теорема о корректности исчисления предикатов). *Любая выводимая формула общезначима.*

Доказательство. Сначала докажем, что все аксиомы общезначимы. Общезначимость (a1) следует из теоремы 1 главы 2. Общезначимость аксиом равенства очевидна. Докажем общезначимость аксиомы (a2).

Итак, пусть $\mathcal{C} \rightleftharpoons \mathcal{A}(t) \supset \exists x\ \mathcal{A}(x)$, причем терм t свободен для переменной x в формуле $\mathcal{A}(x)$. Пусть I — некоторая интерпретация сигнатуры Ω с носителем M, а θ — некоторая оценка формулы $\mathcal{C}$. Требуется доказать, что $I \models \theta\mathcal{C}$. Очевидно, что $\theta\mathcal{C} \rightleftharpoons \theta\mathcal{A}(t) \supset \theta\ \exists x\ \mathcal{A}(x)$. Здесь и далее подстановка считается старшей операцией по отношению к операции оценивания, таким образом, $\theta\mathcal{A}(t)$ — это $\theta\mathcal{B}$ для $\mathcal{B} \rightleftharpoons \mathcal{A}(t)$, а не $\mathcal{C}(t)$ для $\mathcal{C} = \theta\mathcal{A}$. Оценка θ сопоставляет всем свободным переменным формулы $\mathcal{C}$ имена элементов из M. Какие же переменные входят свободно в $\mathcal{C}$? Во-первых, это все свободные переменные формулы $\mathcal{A}(x)$ кроме x. Во-вторых, это все переменные, входящие в терм t (в том числе, возможно, и x). Действительно, поскольку терм t свободен для x в $\mathcal{A}(x)$, переменные, содержащиеся в t, не связываются кванторами формулы $\mathcal{A}(x)$ и остаются свободными в $\mathcal{A}(t)$. Если x входит в θ, то через θ' обозначим оценку, которая получается из θ выбрасыванием столбца, соответствующего переменной x, т. е. θ' сопоставляет всем переменным кроме x те же имена элементов из M, что и θ, а переменной x ничего не сопоставляет. Очевидно, что $\theta\ \exists x\ \mathcal{A}(x) \rightleftharpoons \theta'\ \exists x\ \mathcal{A}(x) \rightleftharpoons \exists x\ \theta'\mathcal{A}(x)$. С другой стороны $\theta\mathcal{A}(t) \rightleftharpoons \theta\mathcal{A}(\theta t)$. Формула $\mathcal{A}(\theta t)$ не содержит свободно x,

так что $\theta\mathcal{A}(\theta t) \rightleftharpoons \theta'\mathcal{A}(\theta t)$. Таким образом, $\theta\mathcal{C} \rightleftharpoons \theta'\mathcal{A}(\theta t) \supset \exists x\ \theta'\mathcal{A}(x)$. Пусть $I \models \theta'\mathcal{A}(\theta t)$, и пусть $c \in M$ есть значение оцененного терма θt. Тогда, очевидно, $I \models \theta'\mathcal{A}(\underline{c})$. По определению истинности это означает, что $I \models \exists x\theta'\mathcal{A}(x)$.

Таким образом, если в интерпретации I истинна посылка формулы $\theta\mathcal{C}$, то истинно и ее заключение, т. е. $I \models \theta\mathcal{C}$, что и требовалось доказать.

Аналогично доказывается общезначимость аксиомы (a3). Докажем общезначимость аксиомы (a4).

Пусть $\mathcal{A}(x)$ и $\mathcal{B}$ — произвольные формулы, причем $\mathcal{B}$ не содержит свободных вхождений переменной x. Очевидно

$$\forall x\ (\mathcal{A}(x) \supset \mathcal{B}) \sim \forall x(\neg\mathcal{A}(x) \vee \mathcal{B}).$$

По теореме 2 из главы 2 имеем

$$\forall x(\neg\mathcal{A}(x) \vee \mathcal{B}) \sim \forall x\neg\mathcal{A}(x) \vee \mathcal{B} \sim \neg\exists x\mathcal{A}(x) \vee \mathcal{B} \sim \exists x\mathcal{A}(x) \supset \mathcal{B}.$$

Мы доказали, что $\forall x(\mathcal{A}(x) \vee \mathcal{B}) \sim \exists x\mathcal{A}(x) \supset \mathcal{B}$. Отсюда следует, что формула $\forall x(\mathcal{A}(x) \vee \mathcal{B}) \supset (\exists x\mathcal{A}(x) \supset \mathcal{B})$ общезначима.

Общезначимость аксиомы (a5) доказывается аналогично.

Теперь докажем, что любая выводимая формула общезначима. Пусть $\mathcal{B}_1, \ldots, \mathcal{B}_n$ — произвольный вывод. Индукцией по i докажем, что формула $\mathcal{B}_i$ общезначима. Если $i = 1$, то $\mathcal{B}_i$ — аксиома, и по доказанному она общезначима. Пусть $i = k + 1$, и для любого $j \leqslant k$ формула $\mathcal{B}_j$ общезначима. Докажем, что $\mathcal{B}_i$ общезначима. По определению вывода формула $\mathcal{B}_i$ получена из формул с меньшими номерами по правилам $(Taut)$ или (Gen). Пусть $\mathcal{B}_i$ получена из формул $\mathcal{B}_{i_1}, \ldots, \mathcal{B}_{i_m}$ по правилу $(Taut)$. По индуктивному предположению $\mathcal{B}_{i_1}, \ldots, \mathcal{B}_{i_m}$ общезначимы. Так как $\mathcal{B}_i$ — их тавтологическое следствие, то по теореме 1 главы 3 $\mathcal{B}_i$ также общезначима.

Пусть формула $\mathcal{B}_i$ получена из формулы $\mathcal{B}_j$, где $j \leqslant k$, по правилу (Gen), т. е. $\mathcal{B}_i \rightleftharpoons \forall x\ \mathcal{B}_j$. Пусть I — произвольная интерпретация с носителем M, а θ — произвольная оценка формулы $\mathcal{B}_i$. Нужно доказать, что $I \models \theta\mathcal{B}_i$. Так как x не входит свободно в $\mathcal{B}_i$, можно считать, что θ не содержит x. Формула $\mathcal{B}_j$ может содержать x свободно, поэтому для нее будем употреблять обозначение $\mathcal{B}_j(x)$. Очевидно, что $\theta\mathcal{B}_i \rightleftharpoons \forall x\theta\mathcal{B}_j(x)$. По индуктивному предположению формула $\mathcal{B}_j(x)$ общезначима, т. е. истинна в I при любой оценке. В частности, если m — произвольный элемент из M, то $I \models \theta'\mathcal{B}_j(x)$, где θ' — оценка, которая всем переменным из θ сопоставляет те же имена, что и θ, и, кроме того, переменной x сопоставляет $\underline{m}$.

Очевидно, что $\theta'\mathcal{B}_j(x) \rightleftharpoons \theta\mathcal{B}_j(\underline{m})$. Таким образом, каков бы ни был элемент $m \in M$, имеет место $I \models \theta\mathcal{B}_j(\underline{m})$. По определению истинности это означает, что $I \models \forall x\theta\mathcal{B}_j(x)$, т. е. $I \models \theta\mathcal{B}_j$, что и требовалось доказать.

Итак, мы доказали, что если последовательность формул $\mathcal{B}_1, \ldots$ $\ldots, \mathcal{B}_n$ является выводом, то все эти формулы общезначимы. Всякая выводимая формула является последней формулой в некотором выводе, следовательно, она тоже общезначима. Теорема доказана.

Теперь можно понять, почему существенно условие, что терм t свободен для x в $\mathcal{A}(x)$ в аксиомах (a2) и (a3). Пусть, например, $\mathcal{A}(x) \rightleftharpoons \forall y\ x = y$, $t \rightleftharpoons y$. Очевидно, что t не свободен для x в $\mathcal{A}(x)$. Имеем: $\mathcal{A}(t) \rightleftharpoons \forall y\ y = y$, $\exists x\mathcal{A}(x) \rightleftharpoons \exists x\ \forall y\ x = y$. Аксиома $(a2)$ принимает вид $\forall y\ y = y \supset \exists x\ \forall y\ x = y$. Очевидно, что эта формула не общезначима. Тот же эффект иллюстрируем на примере аксиомы (a3). Пусть $\mathcal{A}(x) \rightleftharpoons \exists y\ \neg x = y$, $t = y$. Тогда аксиома (a3) примет вид $\forall x\ \exists y \neg x = y \supset \exists y\ \neg y = y$. Эта формула также не общезначима.

Таким образом, если условие, что терм t свободен для x в $\mathcal{A}(x)$, не соблюдается, то аксиомы (a2) и (a3) могут оказаться не общезначимыми.

Также в аксиомах (a4) и (a5) существенно условие, что $\mathcal{B}$ не содержит свободных вхождений x. Например, если $\mathcal{A}(x) \rightleftharpoons P(x)$ и $\mathcal{B} \rightleftharpoons P(x)$, то аксиома $(a4)$ принимает вид

$$\forall x\ (P(x) \supset P(x)) \supset (\exists x P(x) \supset P(x)),$$

а аксиома $(a5)$ — вид

$$\forall x\ (P(x) \supset P(x)) \supset (P(x) \supset \forall x P(x)).$$

Нетрудно проверить, что обе эти формулы не общезначимы.

Правило вывода П называется *производным*, если для каждой фигуры $\dfrac{\mathcal{A}_1, \ldots, \mathcal{A}_n}{\mathcal{A}} \in \Pi$ существует последовательность формул $\mathcal{B}_1, \ldots, \mathcal{B}_k$ такая, что $\mathcal{B}_k \rightleftharpoons \mathcal{A}$, и любая формула в этой последовательности либо является аксиомой, либо принадлежит множеству $\{\mathcal{A}_1, \ldots, \mathcal{A}_n\}$, либо получена из предыдущих по правилам $(Taut)$ или (Gen).

Теорема 5. *Следующие правила вывода являются производными:*

a) $\left\{ \dfrac{\mathcal{B} \supset \mathcal{A}(x)}{\mathcal{B} \supset \forall x\mathcal{A}(x)} \,\middle|\, \begin{array}{l} \mathcal{A}(x) \text{ и } \mathcal{B} \text{ — произвольные формулы, причем} \\ \mathcal{B} \text{ не содержит свободных вхождений } x \end{array} \right\}$;

б) $\left\{ \dfrac{\mathcal{A}(x) \supset \mathcal{B}}{\exists x \mathcal{A}(x) \supset \mathcal{B}} \,\middle|\, \begin{array}{l} \mathcal{A}(x) \text{ и } \mathcal{B} \text{ — произвольные формулы, причем} \\ \mathcal{B} \text{ не содержит свободных вхождений } x \end{array} \right\}$.

Доказательство. Для каждого из этих правил вывода построим требуемую в определении производного правила последовательность формул:

а) 1. $\mathcal{B} \supset \mathcal{A}(x)$;
2. $\forall x\ (\mathcal{B} \supset \mathcal{A}(x))$ (из 1 по (Gen));
3. $\forall x\ (\mathcal{B} \supset \mathcal{A}(x)) \supset (\mathcal{B} \supset \forall x \mathcal{A}(x))$ (аксиома (a5));
4. $\mathcal{B} \supset \forall x \mathcal{A}(x)$ (из 2 и 3 по (MP)).

б) 1. $\mathcal{A}(x) \supset \mathcal{B}$;
2. $\forall x\ (\mathcal{A}(x) \supset \mathcal{B})$ (из 1 по (Gen));
3. $\forall x\ (\mathcal{A}(x) \supset \mathcal{B}) \supset (\exists x \mathcal{A}(x) \supset \mathcal{B})$ (аксиома $(a4)$);
4. $\exists x \mathcal{A}(x) \supset \mathcal{B}$ (из 2 и 3 по (MP)).

Теорема доказана.

Правила а) и б) из теоремы 5 называются *правилами Бернайса.*

При доказательстве выводимости формул можно пользоваться производными правилами вывода. А именно, назовем *сокращенным выводом* любую такую последовательность формул $\mathcal{B}_1, \ldots, \mathcal{B}_n$, что для всех i формула $\mathcal{B}_i$ либо является аксиомой, либо получена из предыдущих формул по правилам $(Taut)$ или (Gen), либо получена из предыдущих формул по какому-либо производному правилу.

Теорема 6. *Если $\mathcal{B}_1, \ldots, \mathcal{B}_n$ — сокращенный вывод, то все формулы $\mathcal{B}_1, \ldots, \mathcal{B}_n$ являются выводимыми.*

Доказательство. Утверждение доказывается индукцией по n. Пусть $n = 1$. Очевидно, если сокращенный вывод состоит из одной формулы, то эта формула — аксиома и потому выводима.

Пусть утверждение верно для любого $n \leqslant k$. Докажем, что оно верно для $n = k + 1$. Итак, пусть $\mathcal{B}_1, \ldots, \mathcal{B}_k, \mathcal{B}_{k+1}$ — сокращенный вывод. Очевидно, что последовательность $\mathcal{B}_1, \ldots, \mathcal{B}_k$ является сокращенным выводом, и по индуктивному предположению все формулы $\mathcal{B}_1, \ldots, \mathcal{B}_k$ выводимы. Докажем, что $\mathcal{B}_{k+1}$ также выводима. Рассмотрим четыре случая, возможные для формулы $\mathcal{B}_{k+1}$ в силу определения сокращенного вывода.

1) $\mathcal{B}_{k+1}$ является аксиомой. В этом случае $\mathcal{B}_{k+1}$ выводима.

2) $\mathcal{B}_{k+1}$ получена из предыдущих формул $\mathcal{B}_{i_1}, \ldots, \mathcal{B}_{i_m}$ по правилу $(Taut)$. Как мы только что доказали, исходя из индуктивного предположения, все формулы $\mathcal{B}_{i_1}, \ldots, \mathcal{B}_{i_m}$ выводимы. Выпишем подряд выводы формул $\mathcal{B}_{i_1}, \ldots, \mathcal{B}_{i_m}$, а затем напишем формулу $\mathcal{B}_{k+1}$. Нетрудно проверить, что полученная последовательность $\ldots, \mathcal{B}_{i_1}, \ldots, \mathcal{B}_{i_m}, \mathcal{B}_{k+1}$ является выводом формулы $\mathcal{B}_{k+1}$.

3) $\mathcal{B}_{k+1}$ получена из некоторой предыдущей формулы $\mathcal{B}_i$ по правилу (Gen). Как и в предыдущем случае, строится вывод формулы $\mathcal{B}_{k+1}$.

4) $\mathcal{B}_{k+1}$ получена из предыдущих формул $\mathcal{B}_{i_1}, \ldots, \mathcal{B}_{i_m}$ по производному правилу вывода. По определению производного правила вывода это означает, что существует последовательность формул $\mathcal{C}_1, \ldots, \mathcal{C}_l$ такая, что $\mathcal{C}_l \rightleftharpoons \mathcal{B}_{k+1}$, и любая формула $\mathcal{C}_i$ либо является аксиомой, либо принадлежит множеству $\{\mathcal{B}_{i_1}, \ldots, \mathcal{B}_{i_m}\}$, либо получена из предыдущих формул по правилу ($Taut$) или (Gen). Все формулы $\mathcal{B}_{i_1}, \ldots, \mathcal{B}_{i_m}$ выводимы. Преобразуем последовательность $\mathcal{C}_1, \ldots, \mathcal{C}_l$ следующим образом: всюду, где в ней встречается какая-нибудь из формул $\mathcal{B}_{i_1}, \ldots, \mathcal{B}_{i_m}$, заменим ее на вывод этой формулы. Очевидно, что полученная последовательность является выводом формулы $\mathcal{B}_{k+1}$. Теорема доказана.

Заметим, что верно и обратное: если все формулы последовательности $\mathcal{B}_1, \ldots, \mathcal{B}_k$ выводимы, то эта последовательность является сокращенным выводом. Действительно, для всех i правило, состоящее из единственной фигуры $\frac{}{\mathcal{B}_i}$, является производным. Таким образом, последовательность $\mathcal{B}_1, \ldots, \mathcal{B}_k$ является сокращенным выводом тогда и только тогда, когда для любого $i \leqslant k$ формула $\mathcal{B}_i$ выводима.

Теорема 7. *Для любой формулы $\mathcal{A}$ выводимы формулы*

$$\neg\exists x\ \mathcal{A} \equiv \forall x\ \neg\mathcal{A};$$
$$\neg\forall x\ \mathcal{A} \equiv \exists x\ \neg\mathcal{A}.$$

Доказательство. Построим сокращенный вывод формулы $\neg\exists x\ \mathcal{A} \equiv \forall x\ \neg\mathcal{A}$.

1. $\mathcal{A} \supset \exists x\ \mathcal{A}$ (аксиома ($a2$));
2. $\neg\exists x\ \mathcal{A} \supset \neg\mathcal{A}$ (из 1. по правилу контрапозиции);
3. $\neg\exists x\ \mathcal{A} \supset \forall x\ \neg\mathcal{A}$ (из 2. по правилу Бернайса);
4. $\forall x\ \neg\mathcal{A} \supset \neg\mathcal{A}$ (аксиома (a3));
5. $\mathcal{A} \supset \neg\forall x\ \neg\mathcal{A}$ (из 4. по правилу контрапозиции);
6. $\exists x\ \mathcal{A} \supset \neg\forall x\ \neg\mathcal{A}$ (из 5. по правилу Бернайса);
7. $\neg\exists x\ \mathcal{A} \equiv \forall x\ \neg\mathcal{A}$ (из 3. и 6. по правилу контрапозиции).

Аналогично доказывается выводимость второй формулы.

Упражнение. Доказать выводимость формул:
а) $\forall x\ \forall y\ P(x,y) \supset \forall y\ \forall x\ P(x,y)$;
б) $\exists x\ \exists y\ P(x,y) \supset \exists y\ \exists x\ P(x,y)$;
в) $\forall x\ P(x) \supset \exists x\ P(x)$;

г) $\forall x\ P(x) \vee \forall x\ Q(x) \supset \forall x\ (P(x) \vee Q(x))$;
д) $\exists x\ (P(x) \,\&\, Q(x)) \supset \exists x\ P(x) \,\&\, \exists x\ Q(x)$;
е) $\forall x\ (P(x) \,\&\, Q(x)) \supset \forall x\ P(x) \,\&\, \forall x\ Q(x)$;
ж) $\exists x\ (P(x) \vee Q(x)) \supset \exists x\ P(x) \vee \exists x\ Q(x)$;
з) $\forall x\ (P(x) \supset Q(x)) \supset (\exists x\ P(x) \supset \exists x\ Q(x))$.

§ 5. Вывод из гипотез

Пусть Γ — произвольное (возможно, бесконечное) множество формул сигнатуры Ω. *Выводом из* Γ называется такая последовательность формул $\mathcal{B}_1, \ldots, \mathcal{B}_n$ сигнатуры Ω, что при любом i ($i = 1, \ldots, n$) формула $\mathcal{B}_i$ либо есть аксиома, либо получена из предыдущих формул по правилу ($Taut$), либо получена из какой-либо предыдущей формулы $\mathcal{A}$ по правилу (Gen), т. е. имеет вид $\forall x\ \mathcal{A}$, причем переменная x не входит свободно ни в одну из формул множества Γ. Будем говорить, что формула $\mathcal{B}$ *выводится из* Γ и писать $\Gamma \vdash B$, если существует такой вывод $\mathcal{B}_1, \ldots, \mathcal{B}_n$ из Γ, что $\mathcal{B}_n \doteqdot \mathcal{B}$.

Таким образом, формулы из Γ при построении вывода из Γ играют ту же роль, что и аксиомы; обычно эти формулы называются *гипотезами*. Очевидно, что если множество гипотез Γ пусто, то определение выводимости из Γ превращается просто в определение выводимости. Условимся вместо $\varnothing \vdash B$ писать $\vdash B$. Заметим, что если в Γ входят только замкнутые формулы, то ограничение на применение правила (Gen) в определении вывода из Γ выполняется автоматически. Вместо $\{\mathcal{A}_1, \ldots, \mathcal{A}_n\} \vdash \mathcal{A}$ будем писать $\mathcal{A}_1, \ldots, \mathcal{A}_n \vdash \mathcal{A}$.

Пример. Докажем, что $P(x)$, $\forall y\ (P(y) \supset Q(y)) \vdash Q(x)$. Действительно, следующая последовательность является выводом:

1. $\forall y\ (P(y) \supset Q(y))$ (гипотеза);
2. $\forall y\ (P(y) \supset Q(y)) \supset (P(x) \supset Q(x))$ (аксиома ($a3$));
3. $P(x) \supset Q(x)$ (из 1. и 2. по (MP));
4. $P(x)$ (гипотеза);
5. $Q(x)$ (из 3. и 4. по (MP)).

Установим некоторые простые, но важные свойства отношения выводимости $\Gamma \vdash \mathcal{B}$.

Теорема 8. *Пусть Γ и Δ — произвольные множества замкнутых формул сигнатуры Ω, причем $\Delta \subseteq \Gamma$. Пусть $\mathcal{B}$ — формула сигнатуры Ω. Тогда, если $\Delta \vdash \mathcal{B}$, то $\Gamma \vdash \mathcal{B}$.*

Доказательство. Пусть $\mathcal{B}_1, \ldots, \mathcal{B}_n$ — вывод формулы $\mathcal{B}$ из Δ. Очевидно, что он является также выводом из Γ. Действительно, каждая из формул $\mathcal{B}_i$ $(i = 1, \ldots, n)$ либо является аксиомой, либо принадлежит Δ (а, значит, и Γ), либо получена по правилам $(Taut)$ или (Gen) из предыдущих формул. Кроме того, поскольку Γ состоит только из замкнутых формул, выполняется ограничение на применение правила (Gen), т.е. выполняются все требования, содержащиеся в определении вывода из Γ. Теорема доказана.

Теорема 9. *Пусть Γ — произвольное (возможно, бесконечное) множество формул сигнатуры Ω, $\mathcal{B}$ — произвольная формула сигнатуры Ω, причем $\Gamma \vdash \mathcal{B}$. Тогда существует такое конечное множество $\Delta \subseteq \Gamma$, что $\Delta \vdash \mathcal{B}$.*

Доказательство. Пусть $\Gamma \vdash \mathcal{B}$. Это означает, что существует такой вывод $\mathcal{B}_1, \ldots, \mathcal{B}_n$ из Γ, что $\mathcal{B}_n \rightleftharpoons \mathcal{B}$. Пусть $\Delta = \{\mathcal{B}_{i_1}, \ldots, \mathcal{B}_{i_m}\}$ — множество всех формул из Γ, входящих в этот вывод. Очевидно, что вывод $\mathcal{B}_1, \ldots, \mathcal{B}_n$ удовлетворяет всем требованиям, содержащимся в определении вывода из Δ. Значит $\mathcal{B}$ выводима из конечного множества $\Delta \subseteq \Gamma$. Теорема доказана.

Теорема 10. *Пусть Γ и Δ — произвольные множества замкнутых формул сигнатуры Ω, причем всякая формула $\mathcal{C} \in \Delta$ выводима из Γ, и пусть $\mathcal{B}$ — произвольная формула сигнатуры Ω и $\Delta \vdash \mathcal{B}$. Тогда $\Gamma \vdash \mathcal{B}$.*

Доказательство. Пусть $\mathcal{B}_1, \ldots, \mathcal{B}_n$ — вывод формулы $\mathcal{B}$ из Δ. Преобразуем его следующим образом. Всюду, где в этом выводе встречается какая-нибудь из формул $\mathcal{C} \in \Delta$, заменим ее на вывод этой формулы из Γ. Нетрудно проверить, что полученная новая последовательность формул является выводом формулы $\mathcal{B}$ из Γ. Теорема доказана.

Теорема 11 (теорема о дедукции). *Если $\Gamma \cup \{\mathcal{A}\} \vdash \mathcal{B}$, то $\Gamma \vdash \mathcal{A} \supset \mathcal{B}$.*

Доказательство. Пусть $\mathcal{B}_1, \ldots, \mathcal{B}_n$ — вывод формулы $\mathcal{B}$ из $\Gamma \cup \{\mathcal{A}\}$. Докажем сначала, что если $\mathcal{B}_i \in \Gamma \cup \{\mathcal{A}\}$ или $\mathcal{B}_i$ — аксиома, то $\Gamma \vdash \mathcal{A} \supset \mathcal{B}_i$. Если $\mathcal{B}_i \in \Gamma$, то $\Gamma \vdash \mathcal{A} \supset \mathcal{B}_i$, так как $\mathcal{A} \supset \mathcal{B}_i$ — тавтологическое следствие формулы $\mathcal{B}_i$. Если же $\mathcal{B}_i \rightleftharpoons \mathcal{A}$, то $\Gamma \vdash \mathcal{A} \supset \mathcal{B}_i$, так как $\mathcal{A} \supset \mathcal{A}$ — тавтология, т.е. аксиома. Если $\mathcal{B}_i$ — аксиома, то $\Gamma \vdash \mathcal{A} \supset \mathcal{B}_i$, так как $\Gamma \vdash \mathcal{B}_i$, и $\mathcal{A} \supset \mathcal{B}_i$ — тавтологическое следствие формулы $\mathcal{B}_i$.

Теперь индукцией по i докажем, что для всех $i \leqslant n$ имеет место $\Gamma \vdash \mathcal{A} \supset \mathcal{B}_i$. Этого достаточно, так как $\mathcal{B} \rightleftharpoons \mathcal{B}_n$.

Пусть $i = 1$. В этом случае $\mathcal{B}_i \in \Gamma \cup \{\mathcal{A}\}$ или $\mathcal{B}_i$ — аксиома, и мы уже доказали, что $\Gamma \vdash \mathcal{A} \supset \mathcal{B}_i$.

Пусть $i = k + 1$, и для любого $j \leqslant k$ имеет место $\Gamma \vdash \mathcal{A} \supset \mathcal{B}_j$. Возможны три случая.

1) $\mathcal{B}_i$ — аксиома или $\mathcal{B}_i \in \Gamma \cup \{\mathcal{A}\}$. В этом случае утверждение уже доказано.

2) $\mathcal{B}_i$ получена из формул $\mathcal{B}_{i_1}, \ldots, \mathcal{B}_{i_m}$ с меньшими номерами применением правила $(Taut)$, т. е. $\mathcal{B}_i$ — тавтологическое следствие формул $\mathcal{B}_{i_1}, \ldots, \mathcal{B}_{i_m}$. Нетрудно проверить, что в этом случае $\mathcal{A} \supset \mathcal{B}_i$ является тавтологическим следствием формул $\mathcal{A}\supset\mathcal{B}_{i_1}, \ldots, \mathcal{A}\supset\mathcal{B}_{i_m}$. По индуктивному предположению $\Gamma \vdash \mathcal{A} \supset \mathcal{B}_{i_1}, \ldots, \Gamma \vdash \mathcal{A} \supset \mathcal{B}_{i_m}$. Выпишем подряд вывод из Γ формул $\mathcal{A} \supset \mathcal{B}_{i_l}$ $(l = 1, \ldots, m)$ и добавим к полученной последовательности формулу $\mathcal{A} \supset \mathcal{B}_i$. Нетрудно проверить, что возникающая при этом последовательность $\ldots, \mathcal{A} \supset \mathcal{B}_{i_1}, \ldots, \mathcal{A} \supset \mathcal{B}_{i_m}, \mathcal{A} \supset \mathcal{B}_i$ является выводом формулы $\mathcal{A} \supset \mathcal{B}_i$ из Γ.

3) $\mathcal{B}_i$ получена из $\mathcal{B}_j$ по правилу (Gen), причем $j \leqslant k$. Тогда $\mathcal{B}_i \leftrightharpoons \forall x\ \mathcal{B}_j$ и x не входит свободно в $\mathcal{A}$ и формулы из Γ. По индуктивному предположению $\Gamma \vdash \mathcal{A} \supset \mathcal{B}_j$. Пусть $\mathcal{C}_1, \ldots, \mathcal{C}_m, \mathcal{A} \supset \mathcal{B}_j$ — вывод формулы $\mathcal{A} \supset \mathcal{B}_j$ из Γ. Дополним эту последовательность следующими формулами: $\forall x\ (\mathcal{A} \supset \mathcal{B}_j)$ (получена из предыдущей по правилу (Gen)); $\forall x\ (\mathcal{A} \supset \mathcal{B}_j) \supset (\mathcal{A} \supset \forall x\ \mathcal{B}_j)$ (аксиома (а5)); $\mathcal{A} \supset \forall x\ \mathcal{B}_j$ (получена из двух предыдущих по правилу (MP)). Полученная последовательность формул очевидно является выводом формулы $\mathcal{A} \supset \forall x\ \mathcal{B}_j$ из Γ. Теорема доказана.

Будем говорить, что множество формул Γ *противоречиво*, и писать $\Gamma \vdash \bot$, если существует такая формула $\mathcal{B}$, что $\Gamma \vdash \mathcal{B}$ и $\Gamma \vdash \neg\mathcal{B}$. В противном случае множество Γ будем называть *непротиворечивым*.

Теорема 12. *а) Если* $\Gamma \vdash \bot$ *и* $\mathcal{C}$ *— любая формула, то* $\Gamma \vdash \mathcal{C}$. *б) Если* $\Gamma, \neg\mathcal{A} \vdash \bot$, *то* $\Gamma \vdash \mathcal{A}$.

Доказательство. а) По условию $\Gamma \vdash \mathcal{B}$ и $\Gamma \vdash \neg\mathcal{B}$ для некоторой формулы $\mathcal{B}$. Выпишем подряд друг за другом выводы формул $\mathcal{B}$ и $\neg\mathcal{B}$ из Γ. К полученной последовательности добавим формулу $\mathcal{C}$. Новая последовательность формул $\ldots, \mathcal{B}, \ldots, \neg\mathcal{B}, \mathcal{C}$ является выводом формулы $\mathcal{C}$ из Γ, поскольку формула $\mathcal{C}$ является тавтологическим следствием формул $\mathcal{B}$ и $\neg\mathcal{B}$.

б) По условию $\Gamma, \neg\mathcal{A} \vdash \mathcal{B}$ и $\Gamma, \neg\mathcal{A} \vdash \neg\mathcal{B}$ для некоторой формулы $\mathcal{B}$. По теореме о дедукции $\Gamma \vdash \neg\mathcal{A} \supset \mathcal{B}$ и $\Gamma \vdash \neg\mathcal{A} \supset \neg\mathcal{B}$. Выпишем подряд друг за другом выводы формул $\neg\mathcal{A} \supset \mathcal{B}$ и $\neg\mathcal{A} \supset \neg\mathcal{B}$ из Γ

и добавим к ним формулу $\mathcal{A}$. Полученная последовательность формул $\ldots, \neg\mathcal{A} \supset \mathcal{B}, \ldots, \neg\mathcal{A} \supset \neg\mathcal{B}, \mathcal{A}$ является выводом формулы $\mathcal{A}$ из Γ, поскольку $\mathcal{A}$ является тавтологическим следствием формул $\neg\mathcal{A} \supset \mathcal{B}$ и $\neg\mathcal{A} \supset \neg\mathcal{B}$. Теорема доказана.

Теорема 13. *Множество замкнутых формул* Γ *непротиворечиво тогда и только тогда, когда любое конечное его подмножество непротиворечиво.*

Доказательство. 1) Докажем, что если множество замкнутых формул Γ непротиворечиво, то любое его подмножество $\Delta \subseteq \Gamma$ непротиворечиво. Пусть Γ непротиворечиво. Допустим, что некоторое его подмножество Δ противоречиво. Это означает, что для некоторой формулы $\mathcal{B}$ имеет место $\Delta \vdash \mathcal{B}$ и $\Delta \vdash \neg\mathcal{B}$. По теореме 8 отсюда следует, что $\Gamma \vdash \mathcal{B}$ и $\Gamma \vdash \neg\mathcal{B}$. Это невозможно в силу предположения о непротиворечивости Γ. Значит, Δ непротиворечиво.

2) Пусть любое конечное подмножество $\Delta \subseteq \Gamma$ непротиворечиво. Допустим, что Γ противоречиво, т. е. для некоторой формулы $\mathcal{B}$ имеет место $\Gamma \vdash \mathcal{B}$ и $\Gamma \vdash \neg\mathcal{B}$. По теореме 9 существуют конечные множества $\Delta_1 \subseteq \Gamma$ и $\Delta_2 \subseteq \Gamma$ такие, что $\Delta_1 \vdash \mathcal{B}$ и $\Delta_2 \vdash \neg\mathcal{B}$. Пусть $\Delta = \Delta_1 \cup \Delta_2$. В силу теоремы 8 $\Delta \vdash \mathcal{B}$ и $\Delta \vdash \neg\mathcal{B}$. Значит, Δ — противоречивое конечное множество. Это противоречит нашему предположению. Значит, Γ непротиворечиво. Теорема доказана.

Упражнение. Доказать, что

а) $\forall x\ (P(x) \supset Q(x)),\ P(y) \vdash Q(y)$;

б) $\forall x\ (P(x) \supset Q(x)),\ \forall x\ P(x) \vdash \forall x\ Q(x)$;

в) $G \vdash \forall x\ \forall z\ \exists y\ x \cdot y = z$;

г) $F \vdash \forall x\ x \cdot 0 = 0$;

д) $F \vdash \forall x\ \forall y\ (x \cdot y = 0 \supset x = 0 \vee y = 0)$,

где G и F — системы аксиом групп и полей соответственно.

§ 6. Теории первого порядка

Пусть нам дана какая-либо система аксиом, т. е. (вообще говоря, произвольное) множество Γ замкнутых формул сигнатуры Ω. Математика интересуют прежде всего те предложения, которые являются логическим следствием аксиом, т. е. такие замкнутые формулы $\mathcal{A}$ сигнатуры Ω, что $\Gamma \models \mathcal{A}$. Следующая теорема показывает, что построение вывода предложения $\mathcal{A}$ из аксиом Γ является одним из способов установления того факта, что $\mathcal{A}$ логически следует из Γ.

Теорема 14 (обобщенная теорема о корректности исчисления предикатов). *Пусть* Γ — *произвольное множество замкнутых формул сигнатуры* Ω, $\mathcal{B}$ — *замкнутая формула той же сигнатуры, причем* $\Gamma \vdash \mathcal{B}$. *Тогда* $\Gamma \models \mathcal{B}$.

Доказательство. Пусть $\Gamma \vdash \mathcal{B}$. По теореме 9 существует конечное множество $\{\mathcal{D}_1, \ldots, \mathcal{D}_m\} \subseteq \Gamma$ такое, что $\mathcal{D}_1, \ldots, \mathcal{D}_m \vdash \mathcal{B}$. Применяя m раз теорему о дедукции, получаем, что формула

$$\mathcal{D}_1 \supset (\mathcal{D}_2 \supset (\ldots \supset (\mathcal{D}_m \supset \mathcal{B}) \ldots))$$

выводима в исчислении предикатов. В силу теоремы о корректности исчисления предикатов (теорема 4) эта формула общезначима, т. е. истинна в любой интерпретации. В частности, если I — произвольная модель множества Γ, то $I \models \mathcal{D}_1 \supset (\mathcal{D}_2 \supset (\ldots \supset (\mathcal{D}_m \supset \mathcal{B}) \ldots))$. Принимая во внимание, что $\mathcal{D}_1, \ldots, \mathcal{D}_m \in \Gamma$, а потому $I \models \mathcal{D}_1, \ldots$ $\ldots, I \models \mathcal{D}_m$, а также определение истинности для формул, имеющих вид импликации, получаем, что $I \models \mathcal{B}$. Значит, $\mathcal{B}$ истинна в любой модели Γ, т. е. $\Gamma \models \mathcal{B}$. Теорема доказана.

Доказанная теорема дает важный способ установления непротиворечивости множества формул.

Теорема 14′. *Пусть множество замкнутых формул* Γ *сигнатуры* Ω *имеет модель. Тогда* Γ *непротиворечиво.*

Доказательство. Пусть Γ имеет модель. Допустим, что множество Γ противоречиво, т. е. для некоторой формулы $\mathcal{A}$ сигнатуры Ω $\Gamma \vdash \mathcal{A}$ и $\Gamma \vdash \neg\mathcal{A}$. Тогда $I \models \mathcal{A}$ и $I \models \neg\mathcal{A}$ по теореме 14. А это невозможно в силу определения истинности. Теорема доказана.

Предъявление вывода формулы $\mathcal{A}$ из множества аксиом Γ можно рассматривать как *доказательство* утверждения $\mathcal{A}$ на основе аксиом, а само предложение $\mathcal{A}$, для которого построен такой вывод, — как *теорему*. Это вполне соответствует представлению о теореме как об утверждении, имеющем доказательство на основе аксиом.

Множество замкнутых формул, которые логически следуют из данного множества аксиом, называется *неформальной аксиоматической теорией* (или *семантической теорией*).

Множество замкнутых формул, которые выводимы в исчислении предикатов из данного множества аксиом, называется *формальной аксиоматической теорией* (или *дедуктивной теорией*).

Множество формул Γ сигнатуры Ω называется *дедуктивно замкнутым*, если для любой замкнутой формулы $\mathcal{B}$ сигнатуры Ω из $\Gamma \vdash \mathcal{B}$ следует $\mathcal{B} \in \Gamma$.

Теорема 15. *Всякая формальная аксиоматическая теория дедуктивно замкнута.*

Доказательство. Пусть Γ — некоторая система аксиом, T — соответствующая ей дедуктивная теория, т.е. множество всех замкнутых формул, выводимых из Γ, и пусть $T \vdash \mathcal{B}$. Мы находимся в условиях теоремы 10: всякая формула из T выводима из Γ, и $T \vdash \mathcal{B}$. В силу этой теоремы $\Gamma \vdash \mathcal{B}$, т.е. $\mathcal{B} \in T$. Теорема доказана.

Теорема 16. *Всякая неформальная аксиоматическая теория дедуктивно замкнута.*

Доказательство. Пусть Γ — некоторая система аксиом, T — соответствующая ей семантическая теория, т.е. множество всех замкнутых формул, логически следующих из Γ, и пусть $T \vdash \mathcal{B}$. По теореме 9 существует конечное множество формул $\{\mathcal{D}_1, \ldots, \mathcal{D}_m\} \subseteq T$ такое, что $\mathcal{D}_1, \ldots, \mathcal{D}_m \vdash \mathcal{B}$. Пусть I — произвольная модель множества Γ. Так как $\mathcal{D}_1, \ldots, \mathcal{D}_m$ принадлежат теории T, то $I \models \mathcal{D}_1, \ldots$ $\ldots, I \models \mathcal{D}_m$, т.е. I — модель множества $\{\mathcal{D}_1, \ldots, \mathcal{D}_m\}$. В силу обобщенной теоремы о корректности исчисления предикатов (теорема 14) $\{\mathcal{D}_1, \ldots, \mathcal{D}_m\} \models \mathcal{B}$. Значит, $I \models \mathcal{B}$. Таким образом, $\mathcal{B}$ истинна в любой модели множества Γ, значит, $\mathcal{B}$ логически следует из Γ, т.е. $\mathcal{B} \in \Gamma$. Теорема доказана.

В силу теоремы 14, если Γ — некоторая система аксиом, T_1 – задаваемая ею дедуктивная теория, а T_2 — соответствующая ей семантическая теория, то $T_1 \subseteq T_2$. Нашей ближайшей целью будет доказательство одной из важнейших теорем математической логики, что $T_1 = T_2$, т.е. что можно говорить об аксиоматической теории, опуская эпитеты “формальная” и “неформальная”.

Как видно из теорем 15 и 16, любая дедуктивная теория и любая семантическая теория дедуктивно замкнуты. Это свойство лежит в основе следующего определения.

Теорией первого порядка (*элементарной теорией* или просто *теорией*) в сигнатуре Ω называется произвольное дедуктивно замкнутое множество замкнутых формул сигнатуры Ω. Таким образом, для теории T утверждения $\mathcal{A} \in T$ и $T \vdash \mathcal{A}$ равносильны.

Семантическая и дедуктивная теории, задаваемые некоторой системой аксиом, — примеры теорий первого порядка. Рассмотрим еще один способ задания теорий, который наряду с аксиоматическим широко используется в математике. А именно, пусть зафиксирована некоторая интерпретация I сигнатуры Ω. Рассмотрим множество $T(I)$ замкнутых формул сигнатуры Ω, истинных в этой интерпретации. Очевидно, что I — модель множества $T(I)$.

Теорема 17. *Какова бы ни была интерпретация I, множество $T(I)$ дедуктивно замкнуто и, следовательно, является теорией первого порядка.*

Доказательство. Докажем, что если замкнутая формула $\mathcal{A}$ сигнатуры Ω такова, что $T(I) \vdash \mathcal{A}$, то $\mathcal{A} \in T(I)$. Пусть $T(I) \vdash \mathcal{A}$. В силу обобщенной теоремы о корректности исчисления предикатов (теорема 14) $T(I) \models \mathcal{A}$, т. е. $\mathcal{A}$ истинна в любой модели множества $T(I)$, в частности, $I \models \mathcal{A}$. Это как раз и означает, что $\mathcal{A} \in T(I)$. Теорема доказана.

Теория $T(I)$ называется *элементарной теорией интерпретации I.* К теориям первого порядка применимо понятие непротиворечивости, введенное нами для произвольных множеств формул. Из теоремы 12 следует, что если теория противоречива, то она содержит все замкнутые формулы данной сигнатуры. Из теоремы 13 непосредственно вытекает, что теория T непротиворечива тогда и только тогда, когда любое конечное множество $\Delta \subseteq T$ непротиворечиво.

Теория первого порядка T в сигнатуре Ω называется *полной* (или *дедуктивно полной*), если T непротиворечива, и для любой замкнутой формулы $\mathcal{A}$ сигнатуры Ω либо $\mathcal{A} \in T$, либо $\neg\mathcal{A} \in T$. В противном случае непротиворечивая теория называется *неполной.*

Теорема 18. *Какова бы ни была интерпретация I, ее элементарная теория $T(I)$ полна.*

Доказательство. Какова бы ни была замкнутая формула $\mathcal{A}$, выполняется ровно одно из условий: $I \models \mathcal{A}$ или $I \not\models \mathcal{A}$ и, значит, $I \models \neg\mathcal{A}$. В первом случае $\mathcal{A} \in T(I)$, во втором — $\neg\mathcal{A} \in T(I)$. Теорема доказана.

Пусть K — некоторый класс интерпретаций сигнатуры Ω. Рассмотрим множество $T(K)$ всех замкнутых формул сигнатуры Ω, истинных в любой интерпретации $I \in K$, т. е. $T(K) = \bigcap_{I \in K} T(I)$. Из теоремы 17 следует, что множество $T(K)$ дедуктивно замкнуто (как пересечение дедуктивно замкнутых множеств). $T(K)$ называется *элементарной теорией класса K*. Очевидно, что если $K_1 \subseteq K_2$, то $T(K_2) \subseteq T(K_1)$. Таким образом, например, элементарная теория групп — это множество предложений языка теории групп, истинных в любой группе. Из дальнейших результатов будет видно, что оно совпадает с множеством предложений, выводимых из аксиом группы.

Заметим, что указанные два способа задания элементарных теорий — аксиоматический и с помощью интерпретаций — принципиально не различаются между собой. Действительно, произвольная элементарная теория может рассматриваться как формальная аксиоматическая теория, аксиомами которой являются все предложения этой теории. В то же время, как следует из теоремы Гёделя, доказанной в гл. 4, любая непротиворечивая теория первого порядка может рассматриваться как элементарная теория некоторого класса интерпретаций, а именно, класса всех ее моделей. Тем не менее, в математической логике очень часто рассматриваются вопросы нахождения простой (например, конечной) аксиоматики для данной теории, если известны все ее модели, а также вопросы описания всех моделей данной аксиоматической теории, т. е. задачи перехода от одного способа задания элементарных теорий к другому. Очень часто эти задачи оказываются весьма содержательными и приводят к глубоким математическим результатам. Позднее мы рассмотрим некоторые из них.

§ 7. Формальная арифметика

Напомним, что описанный нами в § 7 главы 2 язык формальной арифметики имеет сигнатуру, состоящую из единственной константы 0, одноместного функционального символа S и двух двуместных функциональных символов $+$ и $\cdot$. Стандартная интерпретация этого языка имеет своим носителем множество натуральных чисел $\mathbb{N}$, константа 0 и функциональные символы $+$ и $\cdot$ интерпретируются обычным образом, а Sx обозначает $x+1$. Эту интерпретацию обозначим через $\mathfrak{N}$. Очевидно, что с математической точки зрения главный интерес представляет изучение элементарной теории этой интерпретации $T(\mathfrak{N})$, поскольку именно она составляет содержание элементарной теории чисел. Можно сказать, что неявно изучением этой теории и занималась математика, начиная с античных времен.

Аксиоматика арифметики была осуществлена сравнительно недавно. Рассмотрим аксиоматику натурального ряда, предложенную Пеано (1891 г.). Исходные (неопределяемые) понятия этой аксиоматической теории — число 0 и операция перехода от числа n к следующему за ним числу n'.

Аксиомы Пеано:

P1. 0 — натуральное число.

P2. Если n — натуральное число, то n' — натуральное число.

P3. Если m и n — натуральные числа, то $m' = n'$ только в том случае, если $m = n$.

P4. Если n — натуральное число, то $n' \neq 0$.

P5. Пусть P — некоторое свойство натуральных чисел, причем 1) 0 обладает свойством P; 2) если какое-нибудь натуральное число n обладает свойством P, то следующее за ним число n' обладает свойством P. Тогда каждое натуральное число обладает свойством P. Аксиома P5 выражает *принцип математической индукции.*

Попытаемся записать аксиомы Пеано на языке формальной арифметики, добавив к ним еще аксиомы, описывающие свойства сложения и умножения. В результате получим следующую систему аксиом:

A1. $\forall x\ \forall y\ (Sx = Sy \supset x = y)$;

A2. $\forall x\ \neg Sx = 0$;

A3. $\forall x\ x + 0 = x$;

A4. $\forall x\ \forall y\ x + Sy = S(x + y)$;

A5. $\forall x\ x \cdot 0 = 0$,

A6. $\forall x\ \forall y\ x \cdot Sy = x \cdot y + x$,

A7. $\mathcal{A}(0)\ \&\ \forall x\ (\mathcal{A}(x) \supset \mathcal{A}(Sx)) \supset \forall x\ \mathcal{A}(x)$.

Поясним смысл этих аксиом. Аксиомы A1 и A2 выражают соответственно аксиомы Пеано P3 и P4. (Аксиомы Пеано P1 и P2 не нуждаются в специальной записи: их выполнимость обусловлена наличием в языке константы 0 и функционального символа S.) Аксиомы A3–A6 естественным образом задают индуктивные определения операций сложения и умножения. Выражение A7 представляет собой *схему аксиом*: какова бы ни была формула $\mathcal{A}(x)$ языка формальной арифметики, формула вида A7 является аксиомой. Таким образом, A7 представляет бесконечное множество аксиом. Заметим, однако, что схема аксиом A7 не вполне соответствует аксиоме Пеано P5, поскольку последняя распространяется на любое из $2^{\aleph_0}$ свойств натуральных чисел, в то время как схема аксиом A7 имеет дело лишь со счетным числом свойств, записываемых формулами. Тем не менее, схему аксиом A7 принято называть принципом математической индукции.

Задаваемая аксиомами A1–A7 формальная аксиоматическая теория называется *арифметикой Пеано* и обычно обозначается PA. Очевидно, что интерпретация $\mathfrak{N}$ является моделью теории PA, так что $\mathrm{PA} \subseteq T(\mathfrak{N})$. Оказывается, что теории PA и $T(\mathfrak{N})$ не совпадают, т. е. не любая формула, истинная в стандартной интерпретации,

выводима из аксиом теории PA. В этом состоит основное содержание классической теоремы Гёделя о неполноте формальной арифметики.

Эта теорема впоследствии была наполнена следующим более общим смыслом: какова бы ни была система аксиом формальной арифметики, удовлетворяющая некоторым разумным (см. ниже) требованиям, существует истинная в стандартной интерпретации замкнутая формула, не выводимая из этой системы аксиом. “Разумные требования” состоят в следующем: 1) каждая аксиома истинна в стандартной интерпретации; 2) существует алгоритм, распознающий по любой замкнутой формуле рассматриваемой сигнатуры, является ли она аксиомой или нет.

Упражнение. Вывести в PA формулы

$$SS0 + SSS0 = SSSSS0 \quad \text{и} \quad SS0 \cdot SS0 = SSSS0.$$

Г Л А В А 4

ТЕОРЕМА ГЁДЕЛЯ О ПОЛНОТЕ

§ 1. Расширение теории

Цель этой главы — доказать теорему Гёделя о полноте (первая форма) — теорему, обратную к теореме 14′: любое непротиворечивое множество замкнутых формул имеет модель. Достаточно доказать эту теорему только для теорий. Действительно, пусть Γ — произвольное непротиворечивое множество замкнутых формул. Определим T как множество всех замкнутых формул, выводимых из Γ. Тогда T — теория первого порядка, причем T непротиворечива, так как Γ непротиворечиво. Если же T имеет модель, то эта модель является и моделью множества Γ, так как $\Gamma \subseteq T$.

Т е о р е м а 1. *Пусть T — произвольное множество замкнутых формул, $\mathcal{B}$ — замкнутая формула. Множество $T \cup \{\mathcal{B}\}$ непротиворечиво тогда и только тогда, когда $T \nvdash \neg\mathcal{B}$.*

Д о к а з а т е л ь с т в о. Пусть множество $T \cup \{\mathcal{B}\}$ непротиворечиво. Докажем, что $T \nvdash \mathcal{B}$. Допустим обратное: $T \vdash \neg\mathcal{B}$. Тогда по теореме 8 из главы 3 $T \cup \{\mathcal{B}\} \vdash \neg\mathcal{B}$. Кроме того, $T \cup \{\mathcal{B}\} \vdash \mathcal{B}$. Следовательно, множество $T \cup \{\mathcal{B}\}$ противоречиво вопреки предположению.

Пусть множество $T \cup \{\mathcal{B}\}$ противоречиво. По теореме 12 из главы 3 отсюда, в частности, следует, что $T \cup \{\mathcal{B}\} \vdash \neg\mathcal{B}$. По теореме о дедукции $T \vdash \mathcal{B} \supset \neg\mathcal{B}$. Заметим теперь, что $\neg\mathcal{B}$ является тавтологическим следствием формулы $\mathcal{B} \supset \neg\mathcal{B}$, значит $T \vdash \neg\mathcal{B}$. Таким образом, если $T \nvdash \neg\mathcal{B}$, то множество $T \cup \{\mathcal{B}\}$ непротиворечиво. Теорема доказана.

Т е о р е м а 2. *Пусть T — полная теория сигнатуры Ω. Тогда для любых замкнутых формул $\mathcal{A}$ и $\mathcal{B}$ сигнатуры Ω :*

1) $T \vdash \mathcal{A} \,\&\, \mathcal{B} \Leftrightarrow T \vdash \mathcal{A}$ *и* $T \vdash \mathcal{B}$;
2) $T \vdash \mathcal{A} \vee \mathcal{B} \Leftrightarrow T \vdash \mathcal{A}$ *или* $T \vdash \mathcal{B}$;
3) $T \vdash \mathcal{A} \supset \mathcal{B} \Leftrightarrow T \nvdash \mathcal{A}$ *или* $T \vdash \mathcal{B}$;
4) $T \vdash \mathcal{A} \equiv \mathcal{B} \Leftrightarrow (T \vdash \mathcal{A}$ *и* $T \vdash \mathcal{B})$ *или* $(T \nvdash \mathcal{A}$ *и* $T \nvdash \mathcal{B})$.

Д о к а з а т е л ь с т в о. Утверждение 1) очевидно.

Докажем 2). Пусть $T \vdash \mathcal{A} \vee \mathcal{B}$. Докажем, что $T \vdash \mathcal{A}$ или $T \vdash \mathcal{B}$. Допустим противное: $T \nvdash \mathcal{A}$ и $T \nvdash \mathcal{B}$. Тогда в силу полноты T имеем $T \vdash \neg\mathcal{A}$ и $T \vdash \neg\mathcal{B}$. В силу 1) формула $\neg\mathcal{A} \,\&\, \neg\mathcal{B}$ выводима из T. Следовательно, $T \vdash \neg(\mathcal{A} \vee \mathcal{B})$, ибо эта формула есть тавтологическое следствие формулы $\neg\mathcal{A} \,\&\, \neg\mathcal{B}$. Получили, что $T \vdash \mathcal{A} \vee \mathcal{B}$ и $T \vdash \neg(\mathcal{A} \vee \mathcal{B})$. Это невозможно в силу непротиворечивости T. Значит $T \vdash \mathcal{A}$ или $T \vdash \mathcal{B}$.

Пусть $T \vdash \mathcal{A}$ или $T \vdash \mathcal{B}$. Тогда $T \vdash \mathcal{A} \vee \mathcal{B}$, так как $\mathcal{A} \vee \mathcal{B}$ — тавтологическое следствие как формулы $\mathcal{A}$, так и формулы $\mathcal{B}$.

Теперь докажем 3). Пусть $T \vdash \mathcal{A} \supset \mathcal{B}$. Тогда, очевидно, если $T \vdash \mathcal{A}$, то $T \vdash \mathcal{B}$, т.е. или $T \nvdash \mathcal{A}$, или $T \vdash \mathcal{B}$.

Пусть $T \nvdash \mathcal{A}$ или $T \vdash \mathcal{B}$. Если $T \nvdash \mathcal{A}$, то $T \vdash \neg\mathcal{A}$ в силу полноты T, и $T \vdash \mathcal{A} \supset \mathcal{B}$, так как $\mathcal{A} \supset \mathcal{B}$ — тавтологическое следствие $\neg\mathcal{A}$. Аналогично, если $T \vdash \mathcal{B}$, то $T \vdash \mathcal{A} \supset \mathcal{B}$, ибо $\mathcal{A} \supset \mathcal{B}$ — тавтологическое следствие формулы $\mathcal{B}$.

Утверждение 4) доказывается так же, как 2) и 3). Теорема доказана.

Будем говорить, что теория T' является *расширением* теории T, если $T \subseteq T'$.

Следующую теорему называют леммой Линденбаума.

Теорема 3. *Если $S_1 \subseteq S_2 \subseteq \ldots \subseteq S_n \subseteq \ldots$ — возрастающая последовательность непротиворечивых теорий в сигнатуре Ω, то $\bigcup_{n=1}^{\infty} S_n$ есть непротиворечивая теория.*

Доказательство. Докажем сначала, что множество формул $\bigcup_{n=1}^{\infty} S_n$ дедуктивно замкнуто. Пусть $\mathcal{A}$ — замкнутая формула в сигнатуре Ω, причем $\bigcup_{n=1}^{\infty} S_n \vdash \mathcal{A}$. Тогда существует конечное множество $\Gamma \subset \bigcup_{n=1}^{\infty} S_n$, для которого $\Gamma \vdash \mathcal{A}$. В силу конечности Γ существует такое m, что $\Gamma \subset S_m$. Тогда $S_m \vdash \mathcal{A}$, следовательно, $\mathcal{A} \in S_m$ и $\mathcal{A} \in \bigcup_{n=1}^{\infty} S_n$.

Теперь докажем, что множество $\bigcup_{n=1}^{\infty} S_n$ непротиворечиво. Допустим противное: для некоторой формулы $\mathcal{B}$ выполнено $\bigcup_{n=1}^{\infty} S_n \vdash \mathcal{B}$ и $\bigcup_{n=1}^{\infty} S_n \vdash \neg\mathcal{B}$. Тогда существуют конечные $\Gamma_1, \Gamma_2 \subset \bigcup_{n=1}^{\infty} S_n$, для которых $\Gamma_1 \vdash \mathcal{B}, \Gamma_2 \vdash \neg\mathcal{B}$. Вновь существует такое m, что $\Gamma_1 \subset S_m$, $\Gamma_2 \subset S_m$. Следовательно, $S_m \vdash \mathcal{B}$ и $S_m \vdash \neg\mathcal{B}$, что противоречит условию теоремы. Теорема доказана.

Теорема 4 (теорема Линденбаума). *Пусть T — непротиворечивая теория в сигнатуре Ω. Тогда существует полная теория T' в сигнатуре Ω, являющаяся расширением T.*

Доказательство. Докажем теорему в предположении счетности сигнатуры Ω. В общем случае теорема доказывается с использованием аксиомы выбора, точнее, леммы Цорна, эквивалентной аксиоме выбора.

Множество всех замкнутых формул сигнатуры Ω счетно, так как каждая формула сигнатуры Ω является словом в счетном алфавите, полученном добавлением к Ω предметных переменных (их счетное множество) и символов: $=, \neg, \&, \vee, \supset, \equiv, \forall, \exists, (,), ,$, а множество всех слов в любом счетном алфавите счетно.

Пусть $\mathcal{B}_1, \mathcal{B}_2, \ldots, \mathcal{B}_n, \ldots$ — пересчет всех замкнутых формул сигнатуры Ω. Определим последовательность теорий $S_0, S_1, S_2, \ldots$ $\ldots, S_n, \ldots$ следующим образом. Положим $S_0 = T$. Пусть S_n уже определена. Если $\neg\mathcal{B}_{n+1} \in S_n$, то положим $S_{n+1} = S_n$. В этом случае $\neg\mathcal{B}_{n+1} \in S_{n+1}$. Если же $\neg\mathcal{B}_{n+1} \notin S_n$, то пусть S_{n+1} — множество всех замкнутых формул, выводимых из $S_n \cup \{\mathcal{B}_{n+1}\}$. В этом случае $\mathcal{B}_{n+1} \in S_{n+1}$. Определение последовательности $S_0, S_1, S_2, \ldots$ закончено. Очевидно, $S_0, S_1, S_2, \ldots$ — возрастающая последовательность теорий. Докажем индукцией по n, что S_n непротиворечива. При $n = 0$ это нам дано по условию. Пусть $n = k + 1$, и все теории $S_0, S_1, S_2, \ldots, S_k$ непротиворечивы. Если $\neg\mathcal{B}_{k+1} \in S_k$, то $S_{k+1} = S_k$. По индуктивному предположению S_k непротиворечива, следовательно, S_{k+1} непротиворечива. Пусть $\neg\mathcal{B}_{k+1} \notin S_k$. Тогда S_{k+1} есть множество всех замкнутых формул, выводимых из $S_k \cup \{\mathcal{B}_{k+1}\}$. Так как $S_k \nvdash \mathcal{B}_{k+1}$, то по теореме 1 множество $S_k \cup \{\mathcal{B}_{k+1}\}$ непротиворечиво, следовательно, и S_{k+1} непротиворечиво.

Положим $T' = \bigcup_{n=0}^{\infty} S_n$. По лемме Линденбаума (теорема 3) T' — непротиворечивая теория. Докажем, что T' полна. Пусть $\mathcal{B}$ — произвольная формула сигнатуры Ω. Тогда $\mathcal{B}$ имеет некоторый номер в пересчете, скажем, $n + 1$, т. е. $\mathcal{B} \rightleftharpoons \mathcal{B}_{n+1}$. По построению теории S_{n+1} выполнено $\mathcal{B}_{n+1} \in S_{n+1}$ или $\neg\mathcal{B}_{n+1} \in S_{n+1}$. Следовательно, $\mathcal{B}_{n+1} \in T'$ или $\neg\mathcal{B}_{n+1} \in T'$. Теорема доказана.

§ 2. Каноническая интерпретация теории

Пусть T — теория в сигнатуре Ω, содержащей хотя бы одну константу. Определим *каноническую интерпретацию* теории T, которую мы будем обозначать I_0.

Пусть M — множество всех замкнутых термов сигнатуры Ω, т. е. термов, не содержащих переменных. Два замкнутых терма t_1 и t_2

назовем *подобными*, если $T \vdash t_1 = t_2$. Из аксиом равенства (a6)–(a8) следует, что подобие является отношением эквивалентности. Запись $t_1 \sim t_2$ будет означать, что термы t_1 и t_2 подобны.

Определим носитель интерпретации I_0 равным множеству классов эквивалентности замкнутых термов по отношению подобия. Эти классы будем называть далее классами подобия. Класс подобия, содержащий терм t, обозначим $[t]$. Итак, носитель I_0 — это $M_0 = \{[t] \mid t \in M\}$. Теперь определим интерпретацию любой константы $c \in \Omega$, любого функционального символа $f \in \Omega$ и любого предикатного символа $P \in \Omega$.

Положим $\overline{c} = [c]$.

Пусть $[t_1], \ldots, [t_n]$ — произвольные элементы M_0. Тогда $t_1, \ldots$ $\ldots, t_n$ — замкнутые термы. Положим $\overline{f}([t_1], ..., [t_n]) = [f(t_1, ..., t_n)]$. Поскольку $f(t_1, \ldots, t_n)$ и c — замкнутые термы, $[f(t_1, \ldots, t_n)]$ и $[c]$ принадлежат M_0. Заметим, что если $\overline{t}$ — значение замкнутого терма t, то $\overline{t} = [t]$. Действительно, $\overline{c} = c$,

$$\overline{f(t_1, \ldots, t_n)} = \overline{f}(\overline{t}_1, \ldots, \overline{t}_n) = \overline{f}([t_1], \ldots, [t_n]) = [f(t_1, \ldots, t_n)].$$

Положим $\overline{P}([t_1], \ldots, [t_n]) = \text{И} \Leftrightarrow T \vdash P(t_1, \ldots, t_n)$.

Надо показать, что это определение корректно, т. е. что значения $\overline{f}$ и $\overline{P}$ на $[t_1], \ldots, [t_n]$ не зависят от выбора представителей из классов $[t_1], \ldots, [t_n]$. Пусть $[t_1] = [s_1], \ldots, [t_n] = [s_n]$. Требуется доказать, что $[f(t_1, \ldots, t_n)] = [f(s_1, \ldots, s_n)]$ и что $T \vdash P(t_1, \ldots, t_n) \Leftrightarrow$ $\Leftrightarrow T \vdash P(s_1, \ldots, s_n)$. Но это следует непосредственно из аксиом (a9)–(a10) исчисления предикатов.

Определение канонической интерпретации закончено.

Теория T в сигнатуре Ω называется *теорией Генкина*, если для любой замкнутой формулы сигнатуры Ω вида $\exists x \mathcal{A}(x)$ выполнено $T \vdash \mathcal{A}(c)$ для некоторой константы c из Ω, если $T \vdash \exists x \mathcal{A}(x)$.

Мы сначала докажем теорему Гёделя о полноте для полных теорий Генкина, а затем сведем общий случай к этому частному случаю.

Теорема 5. *Пусть T — полная теория Генкина. Тогда каноническая интерпретация теории T является моделью теории T.*

Доказательство. Пусть T — полная теория Генкина в сигнатуре Ω, I_0 — каноническая интерпретация теории T. Индукцией по количеству символов $\exists, \forall, \neg, \&, \vee, \supset, \equiv$ в формуле докажем, что для любой замкнутой формулы $\mathcal{A}$ сигнатуры Ω выполнено $I_0 \models \mathcal{A} \Leftrightarrow$ $\Leftrightarrow T \vdash \mathcal{A}$.

1) Пусть $\mathcal{A} \rightleftharpoons P(t_1, \ldots, t_n)$, где $t_1, \ldots, t_n$ — замкнутые термы. По определению канонической интерпретации

$$\overline{P}([t_1], \ldots, [t_n]) = \text{И} \Leftrightarrow T \vdash P(t_1, \ldots, t_n).$$

Значение любого замкнутого терма t в I_0 равно $[t]$. Таким образом, по определению истинности атомной формулы $P(t_1, \ldots, t_n)$ имеем $I_0 \models P(t_1, \ldots, t_n) \Leftrightarrow \overline{P}([t_1], \ldots, [t_n]) = \text{И}$. Таким образом, $I_0 \models \mathcal{A} \Leftrightarrow$ $\Leftrightarrow T \vdash \mathcal{A}$.

2) Пусть $\mathcal{A} \rightleftharpoons t_1 = t_2$. В этом случае

$$I_0 \models \mathcal{A} \Leftrightarrow I_0 \models t_1 = t_2 \Leftrightarrow [t_1] = [t_2] \Leftrightarrow t_1 \sim t_2 \Leftrightarrow T \vdash \mathcal{A}.$$

3) Пусть $\mathcal{A} \rightleftharpoons \neg\mathcal{B}$. Докажем, что $T \vdash \mathcal{A} \Leftrightarrow I_0 \models \mathcal{A}$. Если $T \vdash \mathcal{A}$, то $T \nvdash \mathcal{B}$, так как T непротиворечива. По индуктивному предположению $I_0 \models \mathcal{B} \Leftrightarrow T \vdash \mathcal{B}$. Значит, $I_0 \not\models \mathcal{B}$. Следовательно, $I_0 \models \mathcal{A}$. Докажем, что $I_0 \models \mathcal{A} \Rightarrow T \vdash \mathcal{A}$. Пусть $I_0 \models \mathcal{A}$, т. е. $I_0 \not\models \mathcal{B}$. По индуктивному предположению $T \nvdash \mathcal{B}$. Тогда $T \vdash \neg\mathcal{B}$ в силу полноты T, т. е. $T \vdash \mathcal{A}$.

Пусть для формул $\mathcal{B}$ и $\mathcal{C}$ доказываемое утверждение верно, т. е. $I_0 \models \mathcal{B} \Leftrightarrow T \vdash \mathcal{B}$ и $I_0 \models \mathcal{C} \Leftrightarrow T \vdash \mathcal{C}$. Докажем это утверждение для формул $\mathcal{B} \vee \mathcal{C}$, $\mathcal{B} \,\&\, \mathcal{C}$, $\mathcal{B} \supset \mathcal{C}$, $\mathcal{B} \equiv \mathcal{C}$.

4) $\mathcal{A} \rightleftharpoons \mathcal{B} \vee \mathcal{C}$. Принимая во внимание теорему 2, индуктивное предположение и определение истинности, получаем:

$$T \vdash \mathcal{A} \Leftrightarrow (T \vdash \mathcal{B} \text{ или } T \vdash \mathcal{C}) \Leftrightarrow (I_0 \models \mathcal{B} \text{ или } I_0 \models \mathcal{C}) \Leftrightarrow I_0 \models \mathcal{A}.$$

5) $\mathcal{A} \rightleftharpoons \mathcal{B} \,\&\, \mathcal{C}$. Аналогично 4), имеем

$$T \vdash \mathcal{A} \Leftrightarrow (T \vdash \mathcal{B} \text{ и } T \vdash \mathcal{C}) \Leftrightarrow (I_0 \models \mathcal{B} \text{ и } I_0 \models \mathcal{C}) \Leftrightarrow I_0 \models \mathcal{A}.$$

6) $\mathcal{A} \rightleftharpoons \mathcal{B} \supset \mathcal{C}$. В этом случае

$$T \vdash \mathcal{A} \Leftrightarrow (T \nvdash \mathcal{B} \text{ или } T \vdash \mathcal{C}) \Leftrightarrow (I_0 \not\models \mathcal{B} \text{ или } I_0 \models \mathcal{C}) \Leftrightarrow I_0 \models \mathcal{A}.$$

7) $\mathcal{A} \rightleftharpoons \mathcal{B} \equiv \mathcal{C}$. Тогда

$$T \vdash \mathcal{A} \Leftrightarrow (T \vdash \mathcal{B} \text{ и } T \vdash C) \text{ или } (T \nvdash \mathcal{B} \text{ и } T \nvdash \mathcal{C}) \Leftrightarrow$$
$$\Leftrightarrow (I_0 \models \mathcal{B} \text{ и } I_0 \models \mathcal{C}) \text{ или } (I_0 \not\models \mathcal{B} \text{ и } I_0 \not\models \mathcal{C}) \Leftrightarrow I_0 \models \mathcal{A}.$$

Пусть для любой замкнутой формулы вида $\mathcal{B}(t)$ верно доказываемое утверждение, т. е. $I_0 \models \mathcal{B}(t) \Leftrightarrow T \vdash \mathcal{B}(t)$. Докажем его для формул $\forall x\, \mathcal{B}(x)$ и $\exists x\, \mathcal{B}(x)$.

8) $\mathcal{A} \rightleftharpoons \exists x\mathcal{B}(x)$. Пусть $T \vdash \mathcal{A}$. Так как T — теория Генкина, то для некоторой константы c из Ω выполнено $T \vdash \mathcal{B}(c)$. По индуктивному предположению $I_0 \models \mathcal{B}(c)$. Следовательно, $I_0 \models \exists x\mathcal{B}(x)$.

Пусть $I_0 \models \exists x\mathcal{B}(x)$, т.е. для некоторого элемента m из носителя I_0 выполнено $I_0 \models \mathcal{B}(\underline{m})$. Но все элементы носителя — классы подобия замкнутых термов. Следовательно, $m = [t]$ для некоторого замкнутого терма t. Тогда для этого терма t выполнено $I_0 \models \mathcal{B}(t)$. По индуктивному предположению отсюда следует $T \vdash \mathcal{B}(t)$. Но $T \vdash \mathcal{B}(t) \supset \exists x\mathcal{B}(x)$ (аксиома (a2)). Следовательно, $T \vdash \exists x\mathcal{B}(x)$.

9) $\mathcal{A} \rightleftharpoons \forall x\mathcal{B}(x)$. Пусть $T \vdash \mathcal{A}$. Для любого замкнутого терма t формула $\forall x\ \mathcal{A}(x) \supset \mathcal{B}(t)$ является аксиомой (a3). Поэтому для любого замкнутого терма t выполнено $T \vdash \mathcal{B}(t)$. По индуктивному предположению из этого следует $I_0 \models \mathcal{B}(t)$ для всех замкнутых термов t. Отсюда и из определения канонической интерпретации вытекает $I_0 \models \forall x\ \mathcal{B}(x)$.

Пусть $I_0 \models \forall x\ \mathcal{B}(x)$. Докажем, что $T \vdash \forall x\ \mathcal{B}(x)$. Допустим противное: $T \nvdash \forall x\mathcal{B}(x)$. Тогда в силу полноты T выполнено $T \vdash \neg\forall x\ \mathcal{B}(x)$. По теореме 7 из главы 3 формула $\neg\forall x\ \mathcal{B}(x) \equiv \exists x\ \neg\mathcal{B}(x)$ выводима в исчислении предикатов, а, значит, и в любой теории. Отсюда получаем, что $T \vdash \exists x\neg\mathcal{B}(x)$. Так как T — теория Генкина, для некоторой константы c мы имеем $T \vdash \neg\mathcal{B}(c)$. С другой стороны, из $I_0 \models \forall x\mathcal{B}(x)$ следует, что $I_0 \models \mathcal{B}(c)$. По индуктивному предположению $T \vdash \mathcal{B}(c)$. Таким образом, $T \vdash \mathcal{B}(c)$ и $T \vdash \neg\mathcal{B}(c)$, что невозможно в силу непротиворечивости T. Значит, предположение $T \nvdash \forall x\ \mathcal{B}(x)$ неверно, и $T \vdash \forall x\ \mathcal{B}(x)$.

Итак, мы доказали, что $I_0 \models \mathcal{A} \Leftrightarrow T \vdash \mathcal{A}$ для любой замкнутой формулы $\mathcal{A}$ сигнатуры Ω. Из этого следует, что все формулы из T истинны в I_0, т.е. I_0 является моделью T.

§ 3. Доказательство теоремы о полноте

Теорема 6 (теорема Генкина). *Пусть T — непротиворечивая теория в сигнатуре Ω. Тогда существуют такие сигнатура $\Omega' \supseteq \Omega$ и теория T' в сигнатуре Ω', что*

1) *T' — расширение теории T;*
2) *T' полна;*
3) *T' — теория Генкина.*

Доказательство. Определим последовательность непротиворечивых теорий $S_0 \subseteq S_1 \subseteq S_2 \subseteq \ldots$ и сигнатур $\Omega_0 \subseteq \Omega_1 \subseteq \Omega_2 \subseteq \ldots$

таких, что S_i — теория в сигнатуре Ω_i. Положим $S_0 = T$, $\Omega_0 = \Omega$. Пусть Ω_n и S_n уже определены. Определим S_{n+1}, Ω_{n+1}.

а) Если n четно, положим $\Omega_{n+1} = \Omega_n$, а S_{n+1} равной любому полному расширению теории S_n в сигнатуре Ω_n. (По теореме Линденбаума (теорема 5) такое расширение существует.)

б) Если n нечетно, то поступаем следующим образом. Для каждой замкнутой формулы $\mathcal{A}$ в сигнатуре Ω_n вида $\exists x\mathcal{B}(x)$, принадлежащей теории S_n, введем новую константу, не содержащуюся в Ω_n. Обозначим эту константу $e_{\mathcal{A}}$ и назовем “свидетелем” формулы $\mathcal{A}$. Для разных формул возьмем разные константы. Положим $\Omega_{n+1} = \Omega_n \cup \{e_{\mathcal{A}} \mid \mathcal{A}$ — замкнутая формула сигнатуры Ω_n вида $\exists x\ \mathcal{B}(x)$ и $\mathcal{A} \in S_n\}$; S_{n+1} — множество замкнутых формул сигнатуры Ω_{n+1}, выводимых из множества $S_n \cup \{\mathcal{B}(e_{\mathcal{A}}) \mid \mathcal{B}(x)$ — формула сигнатуры Ω_n, $\mathcal{A} \rightleftharpoons \exists x\ \mathcal{B}(x)$ — замкнутая формула и $\mathcal{A} \in S_n\}$. Определение S_n и Ω_n закончено.

Лемма 1 (лемма Генкина). *Пусть S — непротиворечивая теория в сигнатуре Ω_n. Тогда множество замкнутых формул сигнатуры Ω_{n+1}, выводимых из множества $S' = S \cup \{\mathcal{B}(e_{\mathcal{A}}) \mid \mathcal{B}(x)$ — формула сигнатуры Ω_n, $\mathcal{A} \rightleftharpoons \exists x\mathcal{B}(x)$ — замкнутая формула и $\mathcal{A} \in S\}$, непротиворечиво.*

Доказательство. Очевидно, достаточно доказать, что само множество S' непротиворечиво. Допустим, что S' противоречиво. В силу теоремы 12 из главы 3 из S' выводима любая формула. В частности, если $\mathcal{D}$ — замкнутая формула сигнатуры Ω_n, то $S' \vdash \mathcal{D}\ \&\ \neg\mathcal{D}$. Фиксируем одну такую формулу $\mathcal{D}$. Пусть $\mathcal{B}_1(e_{\mathcal{A}_1}), \ldots, \mathcal{B}_n(e_{\mathcal{A}_n})$ — все формулы, не принадлежащие S, использованные в выводе из S' формулы $\mathcal{D}\ \&\ \neg\mathcal{D}$. Тогда $S \cup \{\mathcal{B}_1(e_{\mathcal{A}_1}), \ldots, \mathcal{B}_n(e_{\mathcal{A}_n})\} \vdash \mathcal{D}\ \&\ \neg\mathcal{D}$. По теореме о дедукции $S'' \vdash \mathcal{B}_n(e_{\mathcal{A}_n}) \supset \mathcal{D}\ \&\ \neg\mathcal{D}$, где $S'' = S \cup \{\mathcal{B}_1(e_{\mathcal{A}_1}), \ldots, \mathcal{B}_{n-1}(e_{\mathcal{A}_{n-1}})\}$. Пусть $\mathcal{C}_1, \ldots, \mathcal{C}_m$ — вывод формулы $\mathcal{B}_n(e_{\mathcal{A}_n}) \supset \mathcal{D}\ \&\ \neg\mathcal{D}$ из S'', и пусть y — любая переменная, не входящая ни в одну из формул $\mathcal{C}_1, \ldots, \mathcal{C}_m$. Через $\overline{\mathcal{C}_i}$ обозначим формулу, полученную из $\mathcal{C}_i$ заменой всех вхождений константы $e_{\mathcal{A}_n}$ на y. Индукцией по m нетрудно доказать, что последовательность $\overline{\mathcal{C}_1}, \ldots, \overline{\mathcal{C}_m}$ является выводом из S'', но уже формулы $\mathcal{B}_n(y) \supset \mathcal{D}\ \&\ \neg\mathcal{D}$. По правилу Бернайса получаем $S'' \vdash \exists y\ \mathcal{B}_n(y) \supset \mathcal{D}\ \&\ \neg\mathcal{D}$. Нетрудно доказать, что формула $\exists x\ \mathcal{B}_n(x) \equiv \exists y\ \mathcal{B}_n(y)$ выводима в исчислении предикатов. Отсюда получаем $S'' \vdash \exists x\ \mathcal{B}_n(x) \supset \mathcal{D}\ \&\ \neg\mathcal{D}$. Но по условию $S \vdash \exists x\ \mathcal{B}_n(x)$. Так как $S \subset S''$, то $S'' \vdash \exists x\ \mathcal{B}_n(x)$. Значит $S'' \vdash \mathcal{D}\ \&\ \neg\mathcal{D}$.

Применяя описанную процедуру еще $n-1$ раз, мы получим $S \vdash \mathcal{D} \,\&\, \neg\mathcal{D}$, т. е. вопреки условию теория S противоречива. Значит, предположение о противоречивости S' неверно.

Лемма доказана.

Продолжим доказательство теоремы 6.

В силу леммы 1 построенные нами теории $S_0, S_1, \ldots$ непротиворечивы. Положим $\Omega' = \bigcup_{i=0}^{\infty} \Omega_i$, $T' = \bigcup_{i=0}^{\infty} S_i$. По лемме Линденбаума (теорема 3) T' — непротиворечивая теория.

Докажем, что T' полна. Пусть $\mathcal{A}$ — произвольная замкнутая формула сигнатуры Ω'. Тогда $\mathcal{A}$ является формулой сигнатуры Ω_n при некотором n. Очевидно, можно считать, что n четно. По построению теория S_{n+1} полна, следовательно, $\mathcal{A} \in S_{n+1}$ или $\neg\mathcal{A} \in S_{n+1}$. Так как $S_{n+1} \subseteq T'$, то $\mathcal{A} \in T'$ или $\neg\mathcal{A} \in T'$.

Докажем, что T' — теория Генкина. Пусть $\exists x\, \mathcal{B}(x)$ — замкнутая формула, выводимая в T'. Тогда при некотором n формула $\exists x \mathcal{B}(x)$ принадлежит S_n. Очевидно, можно считать, что n нечетно. По построению теории S_{n+1}, в сигнатуре Ω_{n+1} имеется такая константа c, что $\mathcal{B}(c) \in S_{n+1}$. (А именно, в качестве c следует взять $e_{\mathcal{A}}$, где $\mathcal{A} \rightleftharpoons \exists x \mathcal{B}(x)$.) Следовательно, $\mathcal{B}(c) \in T'$, что и требовалось.

Теорема Генкина доказана.

Теорема 7 (теорема Гёделя о полноте). *Любое непротиворечивое множество замкнутых формул имеет модель.*

Доказательство. Пусть T — произвольная непротиворечивая теория. По теореме Генкина (теорема 6) существует полная теория Генкина T', являющаяся расширением теории T. Пусть I — каноническая интерпретация теории T'. По теореме 5 I — модель для T'. Но так как $T \subseteq T'$, интерпретация I является моделью теории T. Теорема доказана.

Отметим важное свойство модели теории T, построенной при доказательстве теоремы Гёделя о полноте.

Теорема 8 (теорема о существовании счетной модели непротиворечивой теории). *Если T — непротиворечивая теория в счетной сигнатуре, то T имеет счетную модель.*

Доказательство. Нетрудно заметить, что если сигнатура Ω счетна, то все сигнатуры $\Omega_1, \Omega_2, \ldots$, построенные в доказательстве теоремы 6, счетны. Следовательно, каноническая интерпретация теории T также счетна. Теорема доказана.

§ 4. Некоторые следствия теоремы Гёделя о полноте

Теорема 9 (вторая форма теоремы Гёделя о полноте). *Пусть $\mathcal{A}$ — общезначимая формула сигнатуры Ω. Тогда $\mathcal{A}$ выводима в исчислении предикатов сигнатуры Ω.*

Доказательство. Достаточно рассмотреть случай, когда $\mathcal{A}$ — замкнутая формула, поскольку всякая формула $\mathcal{A}$, содержащая свободные переменные $x_1, \ldots, x_n$, общезначима тогда и только тогда, когда общезначима формула $\forall x_1 \ldots \forall x_n\ \mathcal{A}$, и выводима тогда и только тогда, когда выводима формула $\forall x_1 \ldots \forall x_n\ \mathcal{A}$. Итак, пусть $\mathcal{A}$ — замкнутая общезначимая формула сигнатуры Ω. Допустим, что $\mathcal{A}$ не выводима в исчислении предикатов. По теореме 12 из главы 3 в этом случае множество $\{\neg\mathcal{A}\}$ непротиворечиво, тогда по теореме Гёделя о полноте (теорема 7) это множество имеет модель, т. е. существует такая интерпретация I, что $I \models \neg\mathcal{A}$. Но это невозможно, поскольку $\mathcal{A}$ общезначима. Значит, формула $\mathcal{A}$ выводима. Теорема доказана.

Теорема 10. *В исчислении предикатов выводимы все общезначимые формулы и только они.*

Доказательство. Это утверждение непосредственно вытекает из теоремы 9 и теоремы о корректности исчисления предикатов (теорема 4 из главы 3).

Теорема 11. *Пусть Γ — произвольное множество замкнутых формул сигнатуры Ω, $\mathcal{B}$ — замкнутая формула сигнатуры Ω, причем $\Gamma \models \mathcal{B}$. Тогда $\Gamma \vdash \mathcal{B}$.*

Доказательство. Пусть $\Gamma \models \mathcal{B}$. Рассмотрим множество формул $\Gamma \cup \{\neg\mathcal{B}\}$. Если бы это множество было непротиворечиво, то по теореме Гёделя о полноте у него существовала бы модель. Но это невозможно, ибо в любой интерпретации, где истинны все формулы из Γ, обязательно истинна формула $\mathcal{B}$, а формула $\neg\mathcal{B}$ ложна. Значит, множество $\Gamma \cup \{\neg\mathcal{B}\}$ противоречиво. По теореме 12 из главы 3 $\Gamma \vdash \mathcal{B}$. Теорема доказана.

Теорема 12. *Замкнутая формула $\mathcal{B}$ является логическим следствием множество замкнутых формул Γ тогда и только тогда, когда $\Gamma \vdash \mathcal{B}$.*

Доказательство. Это утверждение непосредственно вытекает из теоремы 11 и обобщенной теоремы о корректности исчисления предикатов (теорема 14 из главы 3).

Теорема 12 может быть переформулирована так: *неформальная аксиоматическая теория с аксиомами* Γ *совпадает с формальной аксиоматической теорией с аксиомами* Γ. Мы уже объявляли ранее это совпадение, но без доказательства. Теперь мы имеем доказательство.

Теорема 13 (локальная теорема Мальцева). *Пусть* Γ *— произвольное множество замкнутых формул сигнатуры* Ω*, причем любое конечное подмножество* $\Delta \subseteq \Gamma$ *имеет модель. Тогда множество* Γ *имеет модель.*

Доказательство. Достаточно доказать, что множество Γ непротиворечиво, а затем применить теорему Гёделя о полноте. Допустим, что Γ противоречиво. Применяя теорему 13 из главы 3, получаем, что противоречиво некоторое конечное множество $\Delta \subseteq \Gamma$. Но это невозможно, ибо Δ имеет модель. Значит, Γ непротиворечиво и имеет модель. Теорема доказана.

Теорема 14 (теорема Мальцева о компактности). *Пусть* Γ *— произвольное множество замкнутых формул сигнатуры* Ω*,* $\mathcal{B}$ *— произвольная замкнутая формула сигнатуры* Ω*, причем* $\Gamma \models \mathcal{B}$*. Тогда существует такое конечное подмножество* $\Delta \subseteq \Gamma$*, что* $\Delta \models \mathcal{B}$*.*

Доказательство. Пусть $\Gamma \models \mathcal{B}$. В силу теоремы 11 $\Gamma \vdash \mathcal{B}$. По теореме 9 из главы 3 существует конечное множество $\Delta \subseteq \Gamma$ такое, что $\Delta \vdash \mathcal{B}$. Согласно обобщенной теореме о корректности исчисления предикатов $\Delta \models \mathcal{B}$. Теорема доказана.

§ 5. Математические применения теоремы о полноте и ее следствий

Рассмотрим некоторые применения теоремы Гёделя о полноте и ее следствий, значение которых выходит за рамки математической логики.

Пример 1. *Нестандартные модели арифметики.* Пусть T — произвольная теория первого порядка в сигнатуре языка формальной арифметики, причем все формулы из T истинны в стандартной интерпретации $\mathfrak{N}$ этого языка (отсюда, очевидно, следует, что T непротиворечива). Примерами таких теорий являются, в частности, арифметика Пеано PA и $T(\mathfrak{N})$ — элементарная теория интерпретации $\mathfrak{N}$. Сейчас мы докажем, что любая такая теория наряду с $\mathfrak{N}$ имеет и другие, не изоморфные ей, счетные модели. Интерпретации

языка формальной арифметики, не изоморфные $\mathfrak{N}$, называются нестандартными.

Заметим, что в языке формальной арифметики для любого натурального числа n имеется терм $\underline{n}$, значение которого в стандартной интерпретации есть n: $\underline{0} \rightleftharpoons 0$, $\underline{1} \rightleftharpoons S0$, $\underline{2} \rightleftharpoons SS0$, $\ldots$, $\underline{n} \rightleftharpoons \underbrace{SS\ldots S}_{n \text{ раз}}0$.

Расширим сигнатуру языка формальной арифметики, добавив новую константу c. Рассмотрим следующее множество формул этой расширенной сигнатуры:

$$T' = T \cup \{\neg c = \underline{0},\ \neg c = \underline{1},\ \neg c = \underline{2}, \ldots, \neg c = \underline{n},\ \ldots\}.$$

Докажем, что любое конечное подмножество множества T' имеет модель. Пусть Δ — конечное подмножество множества T'. Оно содержит лишь конечное число формул вида $\neg c = \underline{n}$. Пусть это будут формулы $\neg c = \underline{n_1}, \ldots, \neg c = \underline{n_k}$, и пусть m — какое-либо натуральное число, отличное от $n_1, \ldots, n_k$. Дополним стандартную интерпретацию $\mathfrak{N}$ языка формальной арифметики до интерпретации расширенной сигнатуры, положив $\overline{c} = m$. Очевидно, эта интерпретация является моделью множества Δ. Значит, каждое конечное подмножество $\Delta \subseteq T'$ имеет модель. По теореме 13 множество T' имеет модель, следовательно, имеет счетную модель. Обозначим эту модель через $\mathfrak{M}$, а ее носитель — через M. Рассматривая $\mathfrak{M}$ как интерпретацию языка формальной арифметики, нетрудно заметить что $\mathfrak{M}$ является моделью теории T. Докажем, что модели $\mathfrak{M}$ и $\mathfrak{N}$ не изоморфны. А именно, мы докажем, что не существует такого взаимно однозначного соответствия между множествами $\mathbb{N}$ и M, которое сохраняет константу 0 и функциональный символ S. Допустим противное. Пусть $\varphi : \mathbb{N} \to M$ — такое взаимно однозначное соответствие, которое сохраняет 0 и S, т. е. $\varphi 0 = \overline{0}$, $\varphi(n+1) = \overline{S}\varphi n$, где $\overline{0}$ и $\overline{S}$ — соответственно интерпретации константы 0 и символа S в модели $\mathfrak{M}$. Рассмотрим элемент $\overline{c} \in M$, являющийся интерпретацией константы c в модели $\mathfrak{M}$. Поскольку φ — взаимно однозначное соответствие между $\mathbb{N}$ и M, то существует такое $n \in \mathbb{N}$, что $\varphi n = \overline{c}$. С другой стороны, поскольку $n = (\ldots(0 + \underbrace{1) + \ldots + 1) + 1}_{n \text{ раз}})$ и φ сохраняет 0 и S, то $\varphi n = \underbrace{\overline{S}\ldots\overline{S}}_{n \text{ раз}}\overline{0}$. Отсюда получаем, что $\overline{c} = \underbrace{\overline{S}\ldots\overline{S}}_{n \text{ раз}}\overline{0}$, т. е. $\mathfrak{M} \models c = \underline{n}$. Но это невозможно, ибо в $\mathfrak{M}$ истинна формула $\neg c = \underline{n}$. Значит, не существует взаимно однозначное соответствие между $\mathbb{N}$ и $\mathfrak{M}$, сохраняющее 0 и S. Таким образом, модель $\mathfrak{M}$, рассматриваемая как интерпретация языка формальной арифметики, не изоморфна стандартной модели арифметики $\mathfrak{N}$.

Теорема 15. *Существуют счетные нестандартные модели арифметики Пеано PA.*

Доказательство. Это утверждение вытекает из приведенных построений, когда T есть PA.

Теорема 16. *Существует счетная интерпретация, элементарно эквивалентная стандартной интерпретации языка формальной арифметики, но не изоморфная ей.*

Доказательство. Пусть T — есть элементарная теория стандартной интерпретации языка формальной арифметики, то есть $T = T(\mathfrak{N})$. Построенная нами нестандартная модель $\mathfrak{M}$ этой теории элементарно эквивалентна $\mathfrak{N}$. Действительно, какова бы ни была замкнутая формула $\mathcal{B}$ языка формальной арифметики, если $\mathfrak{N} \models \mathcal{B}$, то $\mathcal{B} \in T(\mathfrak{N})$ (по определению теории $T(\mathfrak{N})$) и $\mathfrak{M} \models \mathcal{B}$ (так как $\mathfrak{M}$ — модель теории $T(\mathfrak{N})$). С другой стороны, если $\mathfrak{M} \models \mathcal{B}$, то $\mathcal{B} \in T(\mathfrak{N})$ (так как по теореме 18 из главы 3 теория $T(\mathfrak{N})$ полна, а формула $\neg\mathcal{B}$ ложна в модели $\mathfrak{M}$ теории $T(\mathfrak{N})$) и $\mathfrak{N} \models \mathcal{B}$ (по определению теории $T(\mathfrak{N})$). Теорема доказана.

Теорема 17. *Никакая система аксиом в сигнатуре языка формальной арифметики не задает однозначно, с точностью до изоморфизма, стандартную интерпретацию $\mathfrak{N}$.*

Иными словами, невозможно указать конечную или даже бесконечную систему аксиом, единственной (с точностью до изоморфизма) счетной моделью которой была бы интерпретация $\mathfrak{N}$. Это утверждение немедленно следует из нашего построения нестандартной модели, если в качестве T взять произвольную систему аксиом, истинных в стандартной модели.

Пример 2. *Поля нулевой характеристики.* Обратимся к описанной в § 1 главы 3 системе аксиом для теории полей, которую мы обозначили F. Для каждого поля, т. е. модели этой системы аксиом, однозначно определена его *характеристика.* Это такое простое число p, для которого $p \cdot 1 = 0$, где $p \cdot 1$ есть сокращенное обозначение для суммы p слагаемых $1 + \ldots + 1$. Если же такого числа p нет, то говорят, что поле имеет характеристику 0.

Теорема 18. *Пусть $\mathcal{A}$ — произвольная замкнутая формула в сигнатуре теории полей, истинная во всех полях характеристики* 0. *Тогда существует такое простое число q, что формула $\mathcal{A}$ истинна во всех полях характеристики $\geqslant q$.*

Доказательство. Пусть $\mathcal{A}$ — замкнутая формула, истинная во всех полях характеристики 0. Через $\mathcal{C}_p$ обозначим формулу

$p \cdot 1 = 0$. Рассмотрим множество формул F', полученное присоединением к системе аксиом F формул $\neg\mathcal{C}_p$ для всех простых p, т. е. $F' = F \cup \{\neg\mathcal{C}_2, \ \neg\mathcal{C}_3, \ \neg\mathcal{C}_5, \ \ldots\}$. Любая модель множества F' — это поле характеристики 0, следовательно, в ней истинна формула $\mathcal{A}$. Значит, $F' \models \mathcal{A}$. По теореме о компактности (теорема 14) существует такое конечное множество $\Delta \subseteq F'$, что $\Delta \models \mathcal{A}$. Пусть $\neg\mathcal{C}_{q_1}, \ldots, \neg\mathcal{C}_{q_n}$ — все формулы вида $\neg\mathcal{C}_i$, содержащиеся в Δ, и пусть q — произвольное простое число, большее каждого из чисел $q_1, \ldots, q_n$. Тогда в каждом поле характеристики $\geqslant q$ истинны все формулы из множества Δ, а, значит, и формула $\mathcal{A}$, являющаяся их логическим следствием. Теорема доказана.

Теорема 19. *Понятие поля характеристики* 0 *не может быть задано никаким конечным числом аксиом.*

Доказательство. Любую конечную систему аксиом $\mathcal{A}_1, \ldots$ $\ldots, \mathcal{A}_n$ можно заменить одной аксиомой $\mathcal{A}$ — их конъюнкцией $\mathcal{A}_1 \mathbin{\&} \ldots \mathbin{\&} \mathcal{A}_n$. В силу теоремы 18 эта аксиома не может быть истинной только в полях характеристики 0. Теорема доказана.

Пример 3. *Неразличимость конечного и бесконечного.*

Теорема 20. *Пусть T — произвольная теория первого порядка, причем для любого натурального числа n теория T имеет модель, содержащую не менее n элементов. Тогда теория T имеет бесконечную модель.*

Доказательство. Пусть теория T удовлетворяет условию теоремы. Положим

$$\mathcal{E}_1 \rightleftharpoons \exists x \ x = x;$$

$$\mathcal{E}_2 \rightleftharpoons \exists x_1 \ \exists x_2 \ \neg x_1 = x_2;$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\mathcal{E}_n \rightleftharpoons \exists x_1 \ldots \exists x_n \ (\neg x_1 = x_2 \mathbin{\&} \ldots \mathbin{\&} \neg x_{n-1} = x_n)$$

(т. е. конъюнкция всех формул вида $\neg x_i = x_j$ при $1 \leqslant i < j \leqslant n$). Очевидно, что формула $\mathcal{E}_n$ истинна во всякой интерпретации, содержащей не менее n элементов. Рассмотрим множество формул $T' = T \cup \{\mathcal{E}_1, \mathcal{E}_2, \ldots\}$. Очевидно, что любое конечное подмножество множества T' имеет модель. В силу теоремы 13 множество T' имеет модель, которая не может быть конечной. Эта модель является моделью теории T. Теорема доказана.

Теорема 21. *Не существует замкнутой формулы, истинной во всех конечных интерпретациях данной сигнатуры и ложной во всех бесконечных интерпретациях.*

Доказательство. Допустим, такая формула $\mathcal{A}$ существует. Рассмотрим теорию T, единственной аксиомой которой является $\mathcal{A}$. Эта теория, очевидно, удовлетворяет условию теоремы 20. Следовательно, теория T должна иметь бесконечную модель, т. е. формула $\mathcal{A}$ истинна в некоторой бесконечной интерпретации. Теорема доказана.

§ 6. Категоричность

Пусть $\mathfrak{m}$ — какое-нибудь кардинальное число. Теория первого порядка T называется $\mathfrak{m}$-*категоричной*, если T имеет хотя бы одну модель мощности $\mathfrak{m}$ и любые две ее модели мощности $\mathfrak{m}$ изоморфны.

Пример 1. Рассмотрим сигнатуру, не содержащую никаких констант, функциональных и предикатных символов, и теорию в этой сигнатуре, задаваемую единственной аксиомой $\mathcal{E}_n \,\&\, \neg\mathcal{E}_{n+1}$, где $\mathcal{E}_n$ — формула, построенная в доказательстве теоремы 20. Очевидно, любая модель этой теории содержит ровно n элементов, и все такие модели изоморфны между собой. Значит, эта теория является n-категоричной.

Пример 2. Арифметика Пеано PA и элементарная теория стандартной модели арифметики $T(n)$ не являются $\aleph_0$-категоричными, как следует из существования нестандартных моделей арифметики.

Пример 3. Примером $\aleph_0$-категоричной теории может служить теория плотного линейного порядка без первого и последнего элементов DLO, описанная в § 2 главы 3. Установление изоморфизма между любыми двумя бесконечными счетными плотными линейными порядками без первого и последнего элементов является несложным упражнением.

Упражнения.

1. Доказать $\aleph_0$-категоричность теории DLO.

2. Доказать дедуктивную полноту теории DLO.

Г Л А В А 5

ТЕОРИЯ АЛГОРИТМОВ

§ 1. Вычислимые функции

В наше время, когда об алгоритмах говорят повсюду, понятие алгоритма вряд ли требует объяснения. Первые примеры алгоритмов встречаются уже в начальной школе: алгоритм сложения натуральных чисел столбиком, алгоритм деления с остатком (уголком).

В пунктах 1°–4° мы фиксируем некоторую систему общих понятий, относящихся к алгоритмам.

1°. С каждым алгоритмом связано *множество возможных исходных данных* этого алгоритма. Например, в случае алгоритма сложения столбиком (а также в случае, скажем, алгоритма деления уголком) множество возможных исходных данных есть множество пар натуральных чисел.

2°. Пусть x — возможное исходное данное алгоритма $\mathfrak{A}$. Применим $\mathfrak{A}$ к x; при этом возможны три исхода. 1) Применение $\mathfrak{A}$ к x закончится (в конечное число шагов) и $\mathfrak{A}$ выдаст некоторый *результат* или *ответ*. 2) Применение $\mathfrak{A}$ к x закончится, но безрезультатно. 3) Применение $\mathfrak{A}$ к x вовсе не закончится, т. е. алгоритм будет работать бесконечно. В первом случае будем говорить, что $\mathfrak{A}$ *применим к* x, в двух других случаях будем говорить, что $\mathfrak{A}$ *не применим к* x. То есть, $\mathfrak{A}$ применим к исходному x тогда и только тогда, когда применение $\mathfrak{A}$ к x заканчивается получением результата. Например, алгоритм сложения столбиком применим ко всем возможным исходным данным, результатом будет сумма исходных чисел. Алгоритм деления уголком применим к парам натуральных чисел, в которых вторая компонента не равна нулю. Результатом будет частное и остаток.

Множество тех x, к которым применим $\mathfrak{A}$, будем называть *областью применимости алгоритма.*

В следующем пункте мы определим понятие функции, вычислимой алгоритмом. При этом не всюду применимые алгоритмы будут вычислять не всюду определенные функции.

Частичной функцией из X в Y называется любое множество $A \subseteq X \times Y$ такое, что $\langle x, y_1 \rangle \in A$, $\langle x, y_2 \rangle \in A$ влечет $y_1 = y_2$. В частности, если A пусто, получаем *нигде не определенную функцию.*

В этой главе частичные функции мы будем называть просто функциями. При этом обычные функции из X в Y будем называть всюду определенными функциями.

3°. Пусть $\mathfrak{A}$ — алгоритм, X — множество возможных исходных данных $\mathfrak{A}$, а результаты применения $\mathfrak{A}$ принадлежат множеству Y. Будем говорить, что алгоритм $\mathfrak{A}$ вычисляет частичную функцию f из X в Y, определенную равенством $f(x) \simeq$ (результат применения $\mathfrak{A}$ к x).

Примечание. Знак $\simeq$ называется «условное равенство» и имеет следующий смысл. Если A и B суть какие-то выражения, то $A \simeq B$ есть высказывание, утверждающее, что A и B одновременно определены или не определены и, если определены, то имеют совпадающие значения. Например, высказывание $\frac{x}{x} \simeq \frac{|x|}{|x|}$ истинно, а высказывание $\frac{x}{x} \simeq \frac{|y|}{|y|}$ ложно (здесь x и y — действительные переменные).

Таким образом, вычислимая алгоритмом $\mathfrak{A}$ функция определена на тех $x \in X$, к которым применим $\mathfrak{A}$, причем ее значение на таком x равно результату применения $\mathfrak{A}$ к x, и не определена на тех $x \in X$, к которым $\mathfrak{A}$ не применим. Например, алгоритм сложения столбиком вычисляет всюду определенную функцию $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, $f(x, y) = x + y$. Алгоритм деления уголком вычисляет функцию f из $\mathbb{N} \times \mathbb{N}$ в $\mathbb{N} \times \mathbb{N}$, определенную на тех (m, n), для которых $n \neq 0$, и при $n \neq 0$

$$f(m, n) = (\text{частное от деления } m \text{ на } n, \text{ остаток от деления } m \text{ на } n).$$

Функция называется *вычислимой*, если существует вычисляющий ее алгоритм. Например, функции $x + y$, $x \cdot y$ вычислимы. Композиция вычислимых функций вычислима (покажите это). Нигде не определенная функция вычислима.

4°. Понятие алгоритма имеет смысл, лишь если исходные данные и результаты — «конструктивные объекты». Так, не имеет смысла (во всяком случае без дополнительных уточнений и соглашений) говорить об алгоритме, входом которого является произвольное множество действительных чисел, и даже об алгоритме, входом которого является действительное число. Мы будем избегать таких ситуаций, рассматривая алгоритмы, работающие с *конструктивными объектами*, такими, как натуральные числа, слова в конечном алфавите и т. п. Таким образом, вопрос о вычислимости функции

$f : X \to Y$ осмыслен, лишь если X и Y являются подмножествами «ансамблей конструктивных объектов». Примеры ансамбля конструктивных объектов: множество $\mathbb{N}$ натуральных чисел, множество Б* слов конечного алфавита Б.

В общем понимании, ансамбль — это собрание конструктивных объектов «одного и того же типа». Разумеется, сказанное не является определением в математическом смысле этого слова. Понятие ансамбля конструктивных объектов мы рассматриваем как интуитивное, неопределяемое понятие (так же, как и понятие конструктивного объекта, натурального числа, множества).

Ансамбли обладают свойством: если X и Y — ансамбли, то $X \times Y$ — также ансамбль (наличие у ансамблей этого свойства мы принимаем как аксиому).

Замечание. Часто возникающее заблуждение состоит в том, что для доказательства вычислимости функции f нужно не просто доказать существование вычисляющего ее алгоритма, но и предъявить его. Ничего подобного! Функция

$$f(x) = \begin{cases} 1, & \text{если гипотеза Ферма верна;} \\ 0, & \text{если гипотеза Ферма неверна,} \end{cases}$$

вычислима, так как она равна либо функции, тождественно равной 0, либо функции, тождественно равной 1, а обе они вычислимы.

Задача. Будет ли вычислима функция $f : \mathbb{N} \to \mathbb{N}$, определяемая так: $f(n)$ равно нулю, если в десятичном разложении π есть по крайней мере n девяток подряд, и единице в противном случае?

Если X бесконечно, а Y непусто, то существует невычислимая функция из X в Y. Действительно, множество всех функций из X в Y несчетно (так как множество всех подмножеств X несчетно, а у равных функций равные области определения), а множество всех вычислимых функций из X в Y счетно. Более того, если Y содержит по крайней мере два элемента, то существует всюду определенная невычислимая функция из X в Y (потому что в этом случае уже одно только множество всюду определенных функций несчетно).

§ 2. Разрешимые множества

Буквами X и Y мы будем обозначать ансамбли конструктивных объектов.

Подмножество A ансамбля конструктивных объектов X называют *разрешимым*, если существует алгоритм, который для любого

$x \in X$ отвечает на вопрос «$x \in A$?», т.е. алгоритм, который применим к любому элементу x из X и дает ответ И или Л в зависимости от принадлежности x к A. Другими словами, A разрешимо, если характеристическая функция A

$$\chi_A(x) = \begin{cases} 1, & \text{если } x \in A, \\ 0, & \text{если } x \notin A, \end{cases}$$

вычислима.

Теорема 1. *Пересечение, объединение и дополнение разрешимых множеств разрешимо.*

Доказательство. Пусть $A, B \subseteq X$ — разрешимые множества. Тогда функции $\chi_A(x)$ и $\chi_B(x)$ вычислимы. Характеристическая функция множества $A \cap B$ вычисляется таким алгоритмом: «если $\chi_A(x) = 1$ и $\chi_B(x) = 1$, то $\chi_{A\cap B}(x) = 1$, иначе $\chi_{A\cap B}(x) = 0$»

Функция $\chi_{A\cup B}(x)$ вычисляется алгоритмом: «если $\chi_A(x) = 1$ или $\chi_B(x) = 1$, то $\chi_{A\cup B}(x) = 1$ иначе $\chi_{A\cup B}(x) = 0$».

Наконец, $\chi_{X\setminus A}(x)$ вычисляется алгоритмом: «если $\chi_A(x) = 1$, то $\chi_{X\setminus A}(x) = 0$, иначе $\chi_{X\setminus A}(x) = 1$».

Пример. Разрешимы следующие множества: множество четных чисел, множество простых чисел, множество квадратов натуральных чисел.

Если X бесконечно, то существует неразрешимое подмножество X. Действительно, множество всех подмножеств X несчетно, а множество разрешимых подмножеств счетно, так как счетно множество вычислимых функций. В дальнейшем бесконечность любого ансамбля конструктивных объектов мы примем как аксиому.

§ 3. Полуразрешимые множества

Множество $A \subseteq X$ называется *полуразрешимым*, если существует алгоритм, который применим к элементам A (с каким–то ответом) и не дает ответа на элементах $X \setminus A$. Другими словами, A полуразрешимо, если A есть область определения какой–то вычислимой функции. Очевидно, значения этой функции несущественны, так что (A полуразрешимо) $\leftrightarrow$ (функция f, равная нулю на A и не определенная на $X \setminus A$, вычислима).

Очевидно, не любое множество полуразрешимо, так как если X бесконечно, то множество всех подмножеств X несчетно, а множество полуразрешимых множеств счетно, так как счетно множество алгоритмов.

Теорема 2. *Любое разрешимое множество полуразрешимо.*

Доказательство. Пусть $A \subseteq X$ — разрешимое множество. По определению, χ_A вычислима. Тогда A совпадает с областью применимости следующего алгоритма:

> «если $\chi_A(x) = 1$, то дать ответ 0 и закончить работу, иначе закончить работу, не давая ответа (т. е. безрезультатно)».

Замечание. Как мы увидим позднее, обращение теоремы 2 неверно.

Теорема 3. *Любое конечное подмножество $A \subseteq X$ разрешимо.*

Доказательство. Очевидно.

Мы принимаем в качестве аксиомы, что любой ансамбль конструктивных объектов счетно-бесконечен. Более того, мы принимаем как аксиому следующее свойство ансамблей.

Свойство вычислимой равномощности ансамблей. Если X и Y — два ансамбля, то существует вычислимая биекция $f : X \to Y$.

Пример. Пусть $X = \mathbb{N}$, а Y — множество всех слов в некотором конечном алфавите Б. Тогда построенная нами в первой главе при доказательстве счетности Б* биекция $f : X \to Y$ является вычислимой функцией.

Из свойства вычислимой равномощности следует возможность «перебора всех объектов» любого ансамбля.

Теорема 4. *Для любого ансамбля X существуют такое $x_0 \in X$ и такая вычислимая функция* СЛЕДУЮЩИЙ $: X \to Y$, *что последовательность*

$$\begin{aligned} &x_0, \\ &x_1 = \text{СЛЕДУЮЩИЙ}(x_1), \\ &x_2 = \text{СЛЕДУЮЩИЙ}(x_1), \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{aligned}$$

есть пересчет X без повторений.

Доказательство. По свойству вычислимой равномощности существует вычислимая биекция $g : \mathbb{N} \to X$. Положим $x_0 = g(0)$, СЛЕДУЮЩИЙ$(x) = g(g^{-1}(x) + 1)$. Тогда последовательность $x_0, x_1,$

$x_2, \ldots$ есть просто $g(0), g(1), g(2), \ldots$ (докажите это, воспользовавшись методом математической индукции).

Докажем вычислимость функции СЛЕДУЮЩИЙ. Так как композиция вычислимых функций снова вычислимая функция и так как функция $n+1$ вычислима, достаточно доказать вычислимость функции $g^{-1}(x)$. Значение $g^{-1}(x)$ вычисляется следующим алгоритмом: «перебирать все натуральные числа $n = 0, 1, 2, \ldots$, пока не найдется такое n, что $g(n) = x$; это n выдать в качестве ответа».

Теорема 5. *Если f — (частичная) вычислимая взаимно однозначная функция из X в Y, то f^{-1} — вычислимая взаимно однозначная функция из Y в X.*

Доказательство. Очевидно, что f^{-1} — взаимно однозначная функция из Y в X. Требуется доказать, что f^{-1} вычислима. Значение $f^{-1}(y)$ вычисляется следующим алгоритмом:

> «Перебирать все элементы ансамбля X, пока не найдется такой элемент $x \in X$, что $f(x) = y$. Выдать первый такой элемент x в качестве результата (на самом деле такой x может быть только один).»

Если $y \in \delta_{f^{-1}}$, то такой алгоритм выдаст результат $f^{-1}(y)$, а иначе он будет работать бесконечно долго, перебирая все элементы ансамбля X.

Пусть X и Y — два ансамбля конструктивных объектов. Напомним, что мы приняли как аксиому, что $X \times Y$ — снова ансамбль конструктивных объектов.

Пример. Ансамблями являются $\mathbb{N} \times \mathbb{N}$, $\mathbb{N}^3$, $\mathbb{N} \times \{a, b\}^*$.

Задача. Доказать, что множество

$$\{n \mid (\exists x, y, z \in \mathbb{N})(x, y, z > 0 \,\&\, x^n + y^n = z^n)\}$$

полуразрешимо.

Пусть $A \subseteq X \times Y$.

Первой проекцией (или просто *проекцией*) A называется множество

$$\mathsf{np}\, A = \{x \mid (\exists y \in Y)\langle x, y\rangle \in A\}.$$

Теорема 6. *Проекция разрешимого множества $B \subseteq X \times Y$ полуразрешима.*

Доказательство. Проекция B есть область применимости следующего алгоритма:

«Перебирать все элементы из Y, пока не найдется такой $y \in Y$, что $\langle x, y\rangle \in B$. Если нашелся хотя бы один такой y, то выдать в качестве результата 0».

Заметим, что наш алгоритм будет работать бесконечно, если не существует такого $y \in Y$, что $\langle x, y\rangle \in B$, т.е. если $x \notin \mathsf{np}\, B$, так как перебор элементов Y в этом случае никогда не закончится. Таким образом, алгоритм неприменим ко всем $x \notin \mathsf{np}\, B$. Если же $x \in \mathsf{np}\, B$, то как только перебор дойдет до такого y, что $\langle x, y\rangle \in B$, алгоритм выдаст результат и закончит работу.

Функция $f : \mathbb{N} \to X$ называется *вычислимой последовательностью*, если f — всюду определенная вычислимая функция.

Теорема 7. *Множество значений вычислимой последовательности полуразрешимо.*

Доказательство. Пусть $f : \mathbb{N} \to X$ — вычислимая последовательность. Тогда ρ_f является областью применимости следующего алгоритма:

«Исходное данное: x. Перебирать все натуральные числа, пока не найдется такое $n \in \mathbb{N}$, что $f(n) = x$. Если такое n нашлось, то выдать в качестве результата 0».

§ 4. Свойство пошагового выполнения алгоритма и его следствия

Любой алгоритм работает шагами. Каждый шаг работы алгоритма обязательно заканчивается. Если алгоритм работает бесконечно долго, это означает, что алгоритм делает бесконечное число шагов. Пусть $\mathfrak{A}$ — любой алгоритм, исходными данными которого являются объекты ансамбля X, а значениями — объекты ансамбля Y. Тогда существует алгоритм $\mathfrak{L}$, в следующем смысле информирующий о выполнении $\mathfrak{A}$ по шагам: исходными данными $\mathfrak{L}$ являются пары $\langle x, n\rangle$, $x \in X$, $n \in \mathbb{N}$; алгоритм $\mathfrak{L}$, примененный к паре $\langle x, n\rangle$, сообщает, заканчивается ли применение $\mathfrak{A}$ к x не более, чем за n шагов, и, если да, то каков ответ. Формально, возьмем любой объект, не входящий в Y, обозначим его НЕОПР (не определено). Тогда

$\mathfrak{L}$ на входе пары $\langle x, n\rangle$ дает результат НЕОПР, если применение $\mathfrak{A}$ к X не заканчивается за $\leqslant n$ шагов, и результат y, если применение $\mathfrak{A}$ к x дает y за $\leqslant n$ шагов.

Используя свойство пошагового выполнения, докажем следующее усиление теорем 6 и 7.

Теорема 8. *Следующие свойства подмножества A ансамбля X эквивалентны*:

(1) *A есть область определения некоторой вычислимой функции* (*т. е. A полуразрешимо*);

(2) *A есть проекция некоторого разрешимого множества*;

(3) *$A = \varnothing$ или A есть множество значений некоторой вычислимой последовательности*;

(4) *A есть множество значений некоторой вычислимой функции.*

Доказательство. Мы докажем, что (1) $\to$ (2) $\to$ (3) $\to$ (4) $\to$ (1).

(1) $\to$ (2). Пусть f — вычислимая функция из X в Y, и $A = \delta_f$. Тогда A — проекция разрешимого множества $B = \{\langle x, n\rangle \mid x \in X$, $n \in \mathbb{N}$ и алгоритм, вычисляющий f, в применении к x дает ответ за $\leqslant n$ шагов$\}$.

(2) $\to$ (3). Пусть $B \subseteq X \times Y$ разрешимо и $A = \mathsf{np}\, B$. Если $A = \varnothing$, то доказывать нечего. Поэтому пусть $A \neq \varnothing$. Требуется доказать существование вычислимой последовательности f, для которой $\rho_f = A$. Неформально: нужно по очереди перебирать все элементы ансамбля $X \times Y$, и если n-ый элемент $\langle x_n, y_n\rangle$ ансамбля $X \times Y$ попал в B, то положить $f(n) = x_n$, а иначе положить $f(n)$ равным какому-нибудь фиксированному элементу a_0 из A.

Теперь формально. По свойству вычислимой равномощности ансамблей существует вычислимая биекция $c : \mathbb{N} \to X \times Y$. Обозначим $c(n)$ через $\langle x_n, y_n\rangle$. Зафиксируем некоторый элемент $a_0 \in A$. Тогда A — является множеством значений последовательности, вычисляемой следующим алгоритмом:

«Исходное данное: n; если $\langle x_n, y_n\rangle \in B$, то выдать x_n как ответ, иначе выдать a_0 как ответ».

(3)$\to$(4). Если $A = \varnothing$, то A — множество значений нигде не определенной функции (очевидно, она вычислима). Если A — множество значений вычислимой последовательности, то так как вычислимая последовательность является вычислимой функцией, A удовлетворяет (4).

(4) $\to$ (1). Пусть $A = \rho_f$, где f — функция из Y в X, вычисляемая алгоритмом $\mathfrak{A}$. Требуется построить вычислимую функцию g

с областью определения, равной A. Неформально, $g(x)$ вычисляется алгоритмом:

> «Перебирать все пары $\langle n, y\rangle$, $n \in \mathbb{N}$, $y \in Y$, и для каждой пары $\langle n, y\rangle$ делать n шагов вычисления $f(y)$; как только для хотя бы одной пары будет получен ответ $f(y) = x$, то выдать в качестве результата 0».

Описанный алгоритм не остановится, если нет такого $y \in Y$, что $f(y) = x$ (как нам и нужно), и остановится, если $f(y) = x$ для некоторого y в момент обработки пары $\langle m, y\rangle$, где m — число шагов вычисления $f(y)$.

Формально, A — область применимости следующего алгоритма.

> «Исходное данное: x.
> Перебирать все пары из $\mathbb{N} \times Y$, пока не найдется такая пара $\langle n, y\rangle$, что алгоритм $\mathfrak{A}$ на исходном данном y за $\leqslant n$ шагов дает ответ, равный x; если нашлась хотя бы одна такая пара, то выдать 0 в качестве ответа и закончить работу».

Вспомним, что множество A называется счетным, если $A = \varnothing$ или A есть множество значений некоторой последовательности.

Подмножество A ансамбля X называется *перечислимым*, если $A = \varnothing$ или A есть множество значений некоторой вычислимой последовательности.

Понятие перечислимого множества — вычислимый аналог понятия счетного множества. По теореме 8 множество перечислимо тогда и только тогда, когда оно полуразрешимо. В дальнейшем мы будем употреблять термин «перечислимый» как более традиционный.

Т е о р е м а 9. *Пусть $A \subseteq X$, $B \subseteq X$ — перечислимые множества. Тогда $A \cup B$ и $A \cap B$ — перечислимые множества. Пусть $C \subseteq X \times Y$ перечислимо, тогда* $\mathsf{np}\, C$ *перечислимо.*

Д о к а з а т е л ь с т в о. Докажем, что $A \cup B$ пречислимо. Если хотя бы одно из A, B пусто, то $A \cup B$, очевидно, перечислимо. Пусть $A \neq \varnothing$, $B \neq \varnothing$. Тогда по теореме 8 A и B — множества значений вычислимых последовательностей, скажем f и g. Тогда $A \cup B$ — множество значений последовательности h, определенной так:

$$h(2k) = f(k), \quad h(2k+1) = g(k).$$

Функция $h(k)$ вычисляется алгоритмом:

> «если n четно, то $h(n) = f\left(\frac{n}{2}\right)$, иначе $h(n) = g\left(\frac{n-1}{2}\right)$».

Докажем, что $A \cap B$ перечислимо. Пусть A — область применимости алгоритма $\mathfrak{A}$, а B — область применимости алгоритма $\mathfrak{L}$. Тогда $A \cap B$ — область применимости алгоритма $\mathfrak{I}$:

«Применять $\mathfrak{A}$ к x; если получен результат, то применить $\mathfrak{L}$ к x и в качестве результата выдать результат применения $\mathfrak{L}$ к x».

Если $\mathfrak{A}$ неприменим к x, то $\mathfrak{L}$ не будет применяться к x, следовательно, $\mathfrak{I}$ не даст ответа. Если $\mathfrak{A}$ применим к x, то $\mathfrak{I}$ применим к x тогда и только тогда, когда $\mathfrak{L}$ применим к x.

Докажем, что $\mathsf{np}\,C$ перечислимо. По теореме 8, C есть множество значений некоторой вычислимой функции $f : Z \to X \times Y$. Пусть $g : X \times Y \to X$ — функция взятия первого элемента пары, т. е. $g(\langle x, y\rangle) = x$. Очевидно, g вычислима. Имеем

$$\mathsf{np}\,C = \{x | (\exists y \in X)\langle x, y\rangle \in C\} = \\ = \{g(\langle x, y\rangle) | \langle x, y\rangle \in C\} = \{g(f(z)) | z \in Z\} = \rho_{f\circ g}.$$

Функция $g(f(z))$ вычислима как композиция вычислимых функций.

Теорема 10 (теорема Поста). *Подмножество A ансамбля X разрешимо тогда и только тогда, когда A и $X \setminus A$ перечислимы.*

Доказательство. В одну сторону теорема очевидна. Действительно, если A разрешимо, то и $X \setminus A$ разрешимо и, следовательно, они оба перечислимы.

Обратно, пусть A и $X \setminus A$ перечислимы. Если одно из них пусто, то утверждение очевидно. Пусть A и $X \setminus A$ не пусты. Тогда по любому $x \in X$ можно узнать, принадлежит ли он A, построив вычислимые последовательности, перечисляющие A и $X \setminus A$, и ожидая появления x в одной из них. Формально, если $A = \{f(0), f(1), \ldots\}$, $X \setminus A = \{g(0), g(1), \ldots\}$, то следующий алгоритм отвечает на вопрос «$x \in A$?»

«Исходное данное: x.

Перебирать все натуральные числа, пока не найдется такое n, что $f(n) = x$ или $g(n) = x$. (Из того, что объединение множеств значений f и g равно X, следует, что такое n обязательно найдется, а из того, что $\rho_f \cap \rho_g = \varnothing$, следует, что для этого n будет верно только одно из равенств $f(n) = x$, $g(n) = x$.)

Возьмем первое такое n. Если $f(n) = x$, то $x \in A$, иначе $x \notin A$».

Теорема Поста показывает, что перечислимое неразрешимое множество (которое мы еще построим) обязательно имеет неперечислимое дополнение.

Мы видим, что можно определить разрешимость через перечислимость (теорема Поста). Можно также определить вычислимость через перечислимость. Именно, верен такой факт.

Теорема 11. *Функция f из X в Y вычислима тогда и только тогда, когда ее график $\{\langle x, y\rangle | y = f(x)\}$ — перечислимое подмножество $X \times Y$.*

Доказательство. Пусть f вычислима. Докажем, что ее график — перечислимое множество. Если f нигде не определена, то утверждение очевидно. Пусть $\delta_f \neq \varnothing$. Представим δ_f в виде $\{g(0), g(1), \dots\}$, где g — вычислимая последовательность. Тогда график f есть $\{\langle g(0), f(g(0))\rangle, \langle g(1), f(g(1))\rangle, \dots\}$. Тем самым график f перечислим как множество значений вычислимой функции $h(n) = \langle g(n), f(g(n))\rangle$.

Обратно, пусть график f перечислим. Докажем, что f вычислима. Если график пуст, то f нигде не определена и, очевидно, вычислима. Пусть график f не пуст и есть область значений всюду определенной функции $g : \mathbb{N} \to X \times Y$. Обозначим $g(n)$ через $\langle x_n, y_n\rangle$.

Функция f вычислима таким алгоритмом.

«Исходное данное: x;
Перебирать все $n \in \mathbb{N}$ пока не найдется такое n, что $x_n = x$; если такое n нашлось, то взять первое такое n и в качестве результата выдать y_n».

Отметим, что если $f(x)$ не определено, то алгоритм не заканчивает работу.

Задача. Доказать, что образ и прообраз перечислимого множества при вычислимой функции перечислимы.

Указание. Это легко следует из теоремы о графике, перечислимости пересечения и проекции перечислимых множеств.

Упражнения.

1. Доказать, что непустое множество $A \subseteq \mathbb{N}$ разрешимо тогда и только тогда, когда оно есть множество значений вычислимой возрастающей последовательности.

2. Доказать, что любое бесконечное перечислимое множество включает бесконечное разрешимое подмножество.

3. Доказать, что если множества A и B перечислимы, то существуют перечислимые множества A' и B' такие, что $A' \subseteq A$, $B' \subseteq B$, $A' \cap B' = \varnothing$ и $A' \cup B' = A \cup B$.

§ 5. Универсальная вычислимая функция

Пусть X и Y — ансамбли конструктивных объектов. Будем рассматривать всевозможные алгоритмы, исходными данными для которых являются объекты X, а значения лежат в Y. Обозначим через $Com(X,Y)$ множество всех вычислимых функций из X в Y. Пусть P — некоторый третий ансамбль.

Функция $F\colon P \times X \to Y$ называется *универсальной* для $Com(X,Y)$, если для всех $f \in Com(X,Y)$ найдется такое $p \in P$, что выполнено $(\forall x \in X)\ F(p,x) \simeq f(x)$.

Существование универсальной функции для $Com(X,Y)$ очевидно.

Действительно, множество $Com(X,Y)$, как отмечалось, счетно. Пусть $\{f_0, f_1, f_2, \dots\}$ — пересчет $Com(X,Y)$. Положим $P = \mathbb{N}$ и положим $F(n,x) \simeq f_n(x)$ для всех $n \in \mathbb{N}$, $x \in X$.

Если F — функция из $P \times X$ в Y, а $p \in P$, то через F_p будем обозначать функцию из X в Y, получающуюся из F фиксацией первого аргумента равным p, т. е. $\forall x F_p(x) \simeq F(p,x)$.

Теорема 12 (об универсальной функции). *Для любых ансамблей X и Y существуют ансамбль P и вычислимая функция F из $P \times X$ в Y, универсальная для $Com(X,Y)$.*

Доказательство. Мы постулируем существование алгоритмического языка, на котором можно записать программу любого алгоритма с множеством возможных исходных данных X и результатов из Y. Сами программы будут элементами какого-то ансамбля конструктивных объектов P. Определим $F : P \times X \to Y$ так: $F(p,x) = y \leftrightarrow$ (p есть синтаксически правильная программа, которая на входе x дает результат y). Функция $F(p,x)$ вычислима (вычисляющий ее алгоритм называют *интерпретатором* соответствующего языка программирования). Функция F универсальна. Действительно, пусть $f \in Com(X,Y)$ и f вычисляется алгоритмом $\mathfrak{A}$. Пусть p — программа алгоритма $\mathfrak{A}$. Тогда по определению для всех $x \in X$ $f(x) \simeq F(p,x)$. Теорема доказана.

Пусть F — какая-нибудь функция из $P \times X$ в Y, универсальная для $Com(X,Y)$. Пусть $f \in Com(X,Y)$, а $p \in P$ таково, что

$F_p = f$. Функция F не обязана быть интерпретатором некоторого языка программирования, однако по аналогии мы и в этом случае будем называть p *программой* функции f относительно универсальной функции F. Разумеется, одна и та же функция f может иметь несколько (и даже бесконечно много) программ относительно одной и той же функции F.

Замечание. В теореме об универсальной функции можно ограничиться ансамблем $P = \mathbb{N}$, т. е. справедлива

Теорема 12$'$. *Для любых ансамблей X и Y существует вычислимая функция G из $\mathbb{N} \times X$ в Y, универсальная для $Com(X, Y)$.*

Действительно, по теореме 12, существует ансамбль P и вычислимая универсальная для $Com(X, Y)$ функция F из $P \times X$ в Y. Пусть g — вычислимая биекция из $\mathbb{N}$ в P. Обозначим $g(n)$ через P_n. Положим $G(n, x) \simeq F(P_n, x)$. Тогда, очевидно, G — также универсальная вычислимая функция из $\mathbb{N} \times X$ в Y.

Если G — универсальная функция из $\mathbb{N} \times X$ в Y, а $f \in Com(X, Y)$, то программу f относительно G называют также *номером* f относительно G, а соответствие $n \mapsto G_n$ — *нумерацией* вычислимых функций, соответствующей универсальной функции G.

Пусть G — вычислимая функция из $\mathbb{N} \times \mathbb{N}$ в $\mathbb{N}$, универсальная для класса всех вычислимых функций из $\mathbb{N}$ в $\mathbb{N}$. Построим функцию $f(n) = G(n, n) + 1$. Кажется, что мы пришли к противоречию, так как f — вычислимая функция, отличающаяся от каждой из функций из G_n на аргументе n: $f(n) = G(n, n) + 1 = G_n(n) + 1$. Пусть q — номер функции f относительно нумерации $n \mapsto G_n$. Тогда $G(q, x) = f(x) = G(q, x) + 1$ и $G(q, q) = G(q, q) + 1$.

Разгадка парадокса состоит в том, что значение $G(q, q)$ может быть не определено, и само употребление знака «=» здесь некорректно. А утверждение $G(q, q) \simeq G(q, q) + 1$ как раз и означает, что $G(q, q)$ не определено.

Рассмотрим произвольное всюду определенное продолжение $\overline{f}$ функции f. Мы называем g продолжением h, если из того, что $h(x)$ определено, следует $g(x) = h(x)$. Теперь уже $\overline{f}(n) \not\simeq G_n(n)$: если $G_n(n)$ не определено, то $\overline{f}(n) \not\simeq G_n(n)$ уже потому, что левая часть определена, а правая нет; если же $G_n(n)$ определено, то и $f(n)$ определено и равно $G_n(n)+1$, тогда $\overline{f}(n)$ совпадает с $f(n)$ и не равно $G_n(n)$.

Итак, $\overline{f}$ отлична от всех G_n и, следовательно, невычислима. Мы доказали такой факт:

Теорема 13. *Существует вычислимая функция f из $\mathbb{N}$ в $\mathbb{N}$ не имеющая всюду определенного вычислимого продолжения.*

Теорема 14. *Существует перечислимое неразрешимое множество.*

Доказательство. Пусть A — область определения функции f из теоремы 13. Тогда, по определению, A перечислимо. Докажем от противного, что A неразрешимо. Допустим, A разрешимо. Тогда функция

$$\overline{f}(x) = \begin{cases} f(x), & \text{если } x \in A, \\ 0, & \text{если } x \notin A, \end{cases}$$

— всюду определенное вычислимое продолжение f. Теорема доказана.

Существование перечислимых неразрешимых множеств доказывает, что существуют такие программы p, для которых задача: «определить по данному x, заканчивает ли p работу на x» алгоритмически неразрешима. Тем более неразрешима и общая задача: «определить по данной программе p и входу x, заканчивает ли p работу на x».

Упражнения.

1. Назовем множество $E \subseteq \mathbb{N} \times \mathbb{N}$ *универсальным*, если для любого перечислимого множества $A \subseteq \mathbb{N}$ найдется такое $n \in \mathbb{N}$, что $A = \{x \in \mathbb{N} \mid \langle n, x \rangle \in E\}$. Доказать, что существует перечислимое универсальное множество.

2. Доказать, что любое универсальное множество неразрешимо.

3. Доказать, что существует универсальная вычислимая функция, относительно которой нигде не определенная функция имеет единственный номер.

4. Доказать, что существует бесконечное множество $A \subseteq \mathbb{N}$, не имеющее ни одного бесконечного перечислимого подмножества.

5. Доказать, что существуют непересекающиеся перечислимые множества $A, B \subseteq \mathbb{N}$, для которых не существует разрешимого множества $C \subseteq \mathbb{N}$ такого, что $A \subseteq C$, $B \subseteq \mathbb{N} \setminus C$ (такие перечислимые множества A и B называются *неотделимыми*).

6. Доказать, что существует бесконечное семейство попарно непересекающихся множеств, каждая пара которых неотделима.

7. Доказать, что не существует всюду определенной вычислимой функции, универсальной для семейства всех всюду определенных вычислимых функций.

§ 6. Перечислимость множества теорем

Пусть Ω — сигнатура, состоящая из конечного числа символов. Сопоставим с каждой формулой сигнатуры Ω слово в некотором конечном алфавите, расширяющем Ω. Для этого примем следующее соглашение. До сих пор мы не накладывали ограничений на переменные, используемые в формулах. Теперь договоримся, что разрешается применять только переменные $x_0, x_1, x_2, \ldots$, где индекс может быть равен любому натуральному числу. Тогда любая формула сигнатуры Ω является словом в бесконечном алфавите $\Omega \cup \{=(,)\vee\&\neg\supset\equiv\forall\exists x_0 x_1 x_2 \ldots\}$. Обозначим этот алфавит $\text{Б}_1(\Omega)$. Как видно, все символы из Ω содержатся в $\text{Б}_1(\Omega)$, запятая также содержится в $\text{Б}_1(\Omega)$. Например, любая формула сигнатуры $\{0, S, +, \cdot\}$ является словом в алфавите

$$\{0S{+}{\cdot}{=}(,)\vee\&\neg\supset\equiv\forall\exists x_0 x_1 x_2 \ldots\}.$$

Мы хотим уметь записывать формулы в конечном алфавите. Для этого договоримся переменную x_i записывать словом xu, где u — двоичная запись числа i. Например, x_{19} записывается как $x10011$, а x_0 — как $x0$. Тогда любая формула сигнатуры Ω является словом в алфавите

$$\text{Б}(\Omega) = \Omega \cup \{=(,)\vee\&\neg\supset\equiv\forall\exists x01\}.$$

Например, $\forall x1 \exists x101 P(f(x1, x101))$.

Очевидно, имея произвольное слово в алфавите $\text{Б}(\Omega)$, можно выяснить, является ли оно формулой. Более точно, справедлива

Теорема 15. *Для любой конечной сигнатуры Ω множество формул сигнатуры Ω является разрешимым подмножеством в* $(\text{Б}(\Omega))^*$.

Теория первого порядка называется *разрешимо аксиматизируемой*, если она имеет хотя бы одно разрешимое множество аксиом.

Замечание. Если теория разрешима, то она и разрешимо аксиоматизируема.

Теорема 16. *Множество теорем любой разрешимо аксиоматизируемой теории перечислимо.*

Доказательство. Пусть B — разрешимое множество аксиом теории T. По определению формула A принадлежит T тогда и только тогда, когда имеется вывод $A_1, \ldots, A_n$ из B такой, что $A_n \rightleftharpoons A$. Любая последовательность формул является словом в ал-

фавите Б(Ω), при этом по любым словам u, v можно сказать, является ли u выводом формулы v из B. Точнее, справедлива

Лемма. *Множество* $D = \{\langle u,v\rangle \mid v$ *— формула сигнатуры* Ω, *а* u *— вывод формулы* v *из* $B\}$ *— разрешимое подмножество* $(\text{Б}(\Omega))^* \times (\text{Б}(\Omega))^*$.

Доказательство. Вот алгоритм, отвечающий на вопрос «$\langle u,v\rangle \in D$?».

> «Если u не является последовательностью формул сигнатуры Ω, то ответ = нет. Иначе $u = A_1,\ldots,A_n$ для некоторых формул $A_1,\ldots,A_n$. Для всех i от 1 до n проверяем, верно ли, что A_i — аксиома исчисления предикатов, или $A_i \in B$, или A_i получена из предыдущих формул по одному из правил вывода $(Taut)$, (Gen). Если для хотя бы одного i это не так, то ответ = нет. Иначе смотрим, совпадают ли A_n и v. Если да, то ответ = да, иначе — ответ = нет».

Лемма доказана.

Внимательный читатель, наверное, заметил, что в построении алгоритма мы использовали следующие утверждения:

а) множество конечных последовательностей формул разрешимо (это очевидно);

б) множество аксиом исчисления предикатов разрешимо (это очевидно);

в) множество B разрешимо (это дано);

г) множество $\{\langle C_1,\ldots,C_k,C\rangle | C$ получена из $C_1,\ldots,C_k$ по (Gen) или $(Taut)\}$ разрешимо (это очевидно).

На самом деле, каждое из правил (Gen), $(Taut)$, если его рассматривать как множество кортежей формул, разрешимо.

Из этого замечания следует, что если заменить исчисление предикатов любой другой формальной системой с разрешимым множеством аксиом и конечным числом разрешимых правил вывода, то лемма остается верной.

Продолжим доказательство теоремы. Множество T представимо в виде $T = \{v | (\exists u \in \text{Б}(\Omega)^*)\langle u,v\rangle \in D\}$.

Множество T перечислимо как проекция разрешимого множества. Теорема доказана.

Теорема 16 утверждает, что теория с разрешимым множеством аксиом перечислима. Мы знаем, что существуют перечислимые неразрешимые множества. А существует ли неразрешимая теория

с разрешимым множеством аксиом? А может быть, любая теория неразрешима? На первый вопрос ответ положительный — формальная арифметика неразрешима, а множество ее аксиом, очевидно, разрешимо. Неразрешимость формальной арифметики мы доказывать не будем. На второй вопрос ответ отрицательный — существуют разрешимые теории, например, элементарная теория упорядоченного множества рациональных (или целых) чисел. Это утверждение мы тоже не будем доказывать. Обе эти теории разрешимо аксиоматизируются.

Упражнение. Доказать, что элементарная теория любой конечной интерпретации разрешима и, следовательно, разрешимо аксиоматизируема.

Теорема 17. *Любая полная разрешимо аксиоматизируемая теория разрешима.*

Доказательство. Пусть T — полная теория в сигнатуре Ω с разрешимым множеством аксиом. Тогда, по теореме 16, T перечислима. Дополнение к T также перечислимо, так как для любого слова u алфавита Б(Ω), $u \notin T$ тогда и только тогда, когда слово $\neg u$ принадлежит T или u не является формулой.

По теореме Поста теория T разрешима. Теорема доказана.

§ 7. Машины Тьюринга

Рассмотрим одно из возможных уточнений понятия алгоритма — машины Тьюринга. *Машина Тьюринга* имеет бесконечную вправо *ленту*, разделенную на *ячейки*. В каждой из ячеек может быть записан любой символ из *рабочего алфавита* (или просто — алфавита) машины. Машина имеет *читающе-записывающую головку* и *управляющее устройство* (УУ). Управляющее устройство может находиться в одном из конечного множества *состояний* Q. Множество Q и рабочий алфавит свои для каждой машины Тьюринга. УУ может двигать головку вправо и влево по ленте и записывать в ячейки любой из символов алфавита, при этом прежде записанный символ стирается. Ячейка, на которую смотрит головка, называется *обозреваемой ячейкой*. Действие машины на любом шаге полностью определяется состоянием управляющего устройства и символом в обозреваемой ячейке (*обозреваемым символом*). Это

действие состоит в записывании в обозреваемую ячейку нового символа (возможно, совпадающего со старым) и последующем сдвигании головки вправо или влево на одну ячейку или просто в записи нового символа. То, какое действие нужно предпринять в каждой из возможных ситуаций, записано в программе машины. В множестве состояний выделены два состояния — *начальное* и *заключительное*; будем обозначать их соответственно q_1 и q_0. Будем считать, что алфавит содержит символ 0 (ноль). Если головка находится в крайней левой ячейке, а программа требует сдвига головки влево, то происходит *отказ*, т. е. безрезультатная остановка.

Формально, машина Тьюринга — это тройка $\mathcal{M} = \langle A, Q, P \rangle$, где A — конечное множество такое, что $0 \in A$, Q — конечное множество, не пересекающееся с A и содержащее два выделенных элемента q_0, q_1, а P — это множество выражений одного из трех видов: $qa \to br$, $qa \to bRr$, $qa \to bLr$, где $q, r \in Q$, $a, b \in A$. Элементы множества P называются *командами*, а само множество P — *программой* машины $\mathcal{M}$. Для каждого состояния $q \in Q \setminus \{q_0\}$ и символа $a \in A$ в программе P имеется ровно одна команда с левой частью qa.

Программа указывает, что делать в каждой из возможных ситуаций: если состояние управляющего устройства равно q и $q \neq q_0$, то надо найти команду с левой частью qa, где a — обозреваемый символ (по определению, в программе есть ровно одна такая команда). Если правая часть этой команды есть br, то машина $\mathcal{M}$ записывает в обозреваемую ячейку символ b, и УУ переходит в состояние r. Если правая часть команды есть bRr или bLr, то машина записывает в обозреваемую ячейку символ b, УУ переходит в состояние r, и головка сдвигается на одну ячейку вправо или, соответственно, влево. Если состояние машины $\mathcal{M}$ равно q_0, она заканчивает работу.

Пример 1. Пусть $\mathcal{M} = \langle \{0, 1\}, \{q_0, q_1, q_2\}, P \rangle$, где

$$P = \{q_1 0 \to 0Rq_2,\ q_1 1 \to 1q_0,\ q_2 0 \to 1q_0,\ q_2 1 \to 1Rq_2\}.$$

Проследим работу машины $\mathcal{M}$, начиная с положения

0	0	1	0	1	0	0	0	...
	$\uparrow$							
	q_1							

Вот последовательность действий машины $\mathcal{M}$:

0	0	1	0	1	0	...
		↑				
		q_2				

0	0	1	0	1	0	...
			↑			
			q_2			

0	0	1	1	1	0	...
			↑			
			q_0			

На этом работа машины $\mathcal{M}$ заканчивается, так как УУ пришло в состояние q_0.

Состояние вычисления любой машины Тьюринга на любом его шаге полностью определяется тройкой: (состояние УУ; положение головки на ленте; содержимое ленты, т. е. последовательность символов, записанных в ячейках). Будем считать, что только конечное число ячеек ленты может содержать символ, отличный от 0, т. е. начиная с некоторого места на ленте записаны одни нули. Тройка (состояние УУ; положение головки на ленте; содержимое ленты) называется *конфигурацией* (или машинным словом, мгновенным описанием) машины $\mathcal{M}$. Мы будем записывать конфигурацию в виде слова uqv, где q — состояние управляющего устройства, u — слово, записанное на ленте в ячейках до обозреваемой ячейки (исключая ее саму), а v — слово, записанное в ячейках, начиная с обозреваемой и до любого такого места, после которого идут уже одни нули. Таким образом, слово v не определяется однозначно конфигурацией. Например, конфигурацию

0	a	b	c	b	a	0	1	0	0	...
			↑							
			q							

можно записать как в виде слова $0abqcba010$, так и в виде слова $0abqcba0100$.

Последовательность конфигураций из примера 1 можно изобразить так: $0q_10101$, $00q_2101$, $001q_201$, $001q_011$.

Пусть k — конфигурация некоторой машины $\mathcal{M}$. Обозначим через k' конфигурацию, в которую $\mathcal{M}$ переходит из конфигурации k за один шаг. Конфигурация k' определена, если состояние в конфигурации k не равно q_0, и программа не требует сдвига за край ленты. Будем говорить, что $\mathcal{M}$ *перерабатывает* конфигурацию k в конфигурацию l и писать $k \Rightarrow_{\mathcal{M}} l$, если существуют конфигурации $k_0, k_1, \ldots, k_t$ такие, что $k_0 = k$, $k_t = l$, и для всех $i < t$ $k_{i+1} = (k_i)'$. Иными словами, $\mathcal{M}$ перерабатывает конфигурацию k в конфигурацию l, если l получается из k за несколько шагов работы машины $\mathcal{M}$.

Пусть $\mathcal{M}$ — машина Тьюринга с алфавитом A, а u — слово в алфавите A. Назовем конфигурацию $q_1 0u$ *начальной конфигурацией* (или начальным положением) на исходном данном (*входе*) u. Таким образом, в начальной конфигурации на исходном данном u на ленте написано слово $0u$, а дальше — одни нули, головка смотрит на первый символ, УУ находится в начальном состоянии. Последовательность конфигураций $k_0 = q_1 0u$, $k_1 = (q_1 0u)'$, $k_2 = (k_1)', \ldots$, получающуюся при работе машины $\mathcal{M}$ на начальной конфигурации $q_1 0u$, назовем *вычислением* машины $\mathcal{M}$ на входе u. Формально, вычисление на входе u — это конечная или бесконечная последовательность конфигураций $k_0, k_1, \ldots$ такая, что $k_0 = q_1 0u$, и для всех $n \geqslant 0$ либо конфигурация $(k_n)'$ не определена, и k_n — последний член последовательности, либо конфигурация $(k_n)'$ определена и равна k_{n+1}.

Если вычисление на входе u конечно, то будем говорить, что машина Тьюринга $\mathcal{M}$ *останавливается* на входе u. Если $\mathcal{M}$ останавливается на входе u, то в последней конфигурации либо $\mathcal{M}$ находится в состоянии q_0, либо происходит отказ, т. е. программа требует выхода за край ленты. В случае отказа вычисление считается *безрезультатным.* Возможны различные договоренности, что считать результатом вычисления в том случае, когда машина остановилась в состоянии q_0. Пусть в качестве результатов вычисления рассматриваются только слова в алфавите Δ, включенном в алфавит машины $\mathcal{M}$ и не содержащем символа 0. Слово $v \in \Delta^*$ будем называть *результатом вычисления в сильном смысле*, если вычисление конечно, и последняя конфигурация может быть записана в виде слова $q_0 0v$. Непустое слово $v \in \Delta^*$ будем называть *результатом вычисления в слабом смысле*, если вычисление конечно, и последняя конфигурация имеет вид $w_1 \alpha v_1 q_0 v_2 \beta w_2$, где $v_1 v_2 = v$, причем $v_2 \neq \Lambda$, $\alpha, \beta \notin \Delta$. Пустое слово $\Lambda \in \Delta^*$ будем считать результатом вычисления в слабом смысле, если вычисление конечно, и последняя конфигурация имеет вид $w_1 q_0 \beta w_2$, где $\beta \notin \Delta$. Заметим, что

результат вычисления в слабом смысле существует всегда, когда машина завершает работу в состоянии q_0.

Пусть Σ и Δ — произвольные алфавиты такие, что $0 \notin \Sigma$, $0 \notin \Delta$, и пусть f — частичная функция из Σ^* в Δ^*, а $\mathcal{M}$ — машина Тьюринга с алфавитом, включающим алфавиты Σ и Δ. Будем говорить, что машина $\mathcal{M}$ *вычисляет функцию f в слабом (сильном) смысле*, если для всех $u \in \Sigma^*$, $v \in \Delta^*$ вычисление машины $\mathcal{M}$ на входе u завершается остановкой с результатом вычисления в слабом (сильном) смысле v тогда и только тогда, когда $f(u) = v$. Иными словами, если машина $\mathcal{M}$ вычисляет функцию f (в слабом или сильном смысле), и значение $f(u)$ определено, то вычисление машины $\mathcal{M}$ на входе u завершается остановкой с результатом $f(u)$ (соответственно в слабом или сильном смысле). Если же значение $f(u)$ не определено, и машина $\mathcal{M}$ вычисляет функцию f в слабом смысле, то вычисление машины $\mathcal{M}$ на входе u либо вовсе не заканчивается, либо завершается отказом. Если же машина $\mathcal{M}$ вычисляет функцию f в сильном смысле, и значение $f(u)$ не определено, то вычисление машины $\mathcal{M}$ на входе u либо вовсе не заканчивается, либо завершается отказом, либо завершается остановкой в состоянии q_0, но никакое слово в алфавите Δ не является результатом вычисления в сильном смысле.

Функция f из Σ^* в Δ^* называется *вычислимой по Тьюрингу в слабом (сильном) смысле*, если существует машина Тьюринга, которая вычисляет функцию f в слабом (соответственно, сильном) смысле. Заметим, что рабочий алфавит машины $\mathcal{M}$, вычисляющей функцию f из Σ^* в Δ^*, может быть шире, чем алфавит $\Sigma \cup \Delta \cup \{0\}$.

Пример 2. Пусть функция f из $\{a, b\}^*$ в $\{a, b\}^*$ определена равенством

$$f(u) \simeq \begin{cases} \Lambda, & \text{если число букв } a \text{ в слове } u \text{ четно;} \\ \text{не определено в противном случае.} \end{cases}$$

Функция f вычисляется в сильном смысле машиной Тьюринга $\mathcal{M}$ с алфавитом $\{\#, 0, a, b\}$, состояниями q_0, q_1, q_2, q_3, q_4 и следующими командами:

$$q_1 0 \to \# R q_2$$
$$q_2 a \to 0 R q_3$$
$$q_2 b \to 0 R q_2$$
$$q_3 a \to 0 R q_2$$

$$q_3 b \to 0Rq_3$$
$$q_2 0 \to 0Lq_4$$
$$q_3 0 \to 0q_3$$
$$q_4 0 \to 0Lq_4$$
$$q_4 \# \to 0q_0$$

Недостающие команды с левыми частями $q_1 a$, $q_1 b$, $q_1 \#$, $q_2 \#$, $q_3 \#$ и т. д. можно взять произвольно. Машина $\mathcal{M}$, начиная работу на входе u, записывает символ $\#$ в первую ячейку ленты и затем двигает головку по слову u, стирая его буквы. При этом движении машина $\mathcal{M}$ находится в состоянии q_2, если число букв a в прочитанной части слова u четно, и в состоянии q_3, если это число нечетно (обозреваемая ячейка прочитанной не считается). Прочитав слово u, т. е. дойдя до первого символа 0 справа, машина $\mathcal{M}$ «зацикливается», если она находится в состоянии q_3, и начинает движение влево, если она находится в состоянии q_2 (т. е. число букв a четно). Дойдя до символа $\#$, машина $\mathcal{M}$ заменяет его на 0 и заканчивает работу. При этом на ленте записаны одни нули, т. е. результат в сильном смысле равен пустому слову.

А вот пример машины Тьюринга, вычисляющей ту же функцию f в слабом смысле. Пусть машина Тьюринга $\mathcal{M}'$ имеет алфавит $\{0, a, b\}$, состояния q_0, q_1, q_2, q_3, а ее программа состоит из следующих команд:

$$q_1 0 \to 0Rq_2$$
$$q_2 a \to 0Rq_3$$
$$q_2 b \to 0Rq_2$$
$$q_2 0 \to 0q_0$$
$$q_3 a \to 0Rq_2$$
$$q_3 b \to 0Rq_3$$
$$q_3 0 \to 0q_3$$

Недостающие команды с левыми частями $q_1 a$ и $q_1 b$ можно взять произвольно. Машина $\mathcal{M}'$, начиная работу на входе u, двигает головку по слову u, стирая его буквы. При этом она находится в состоянии q_2, если число букв a в прочитанной части слова u четно, и в состоянии q_3, если это число нечетно. Прочитав слово u, т. е. дойдя до первого символа 0 справа, машина $\mathcal{M}'$ «зацикливается», если она находится в состоянии q_3, и останавливается в состоянии q_0, если

она находится в состоянии q_2 (т.е. число букв a четно). При этом в обозреваемой ячейке записан символ 0, т.е. результат в слабом смысле равен пустому слову.

Теорема 18. *Если частичная функция f из Σ^* в Δ^* вычислима по Тьюрингу в сильном смысле, то существует машина Тьюринга, вычисляющая функцию f в сильном смысле, которая работает бесконечно долго на всех входах $u \in \Sigma^*$, для которых значение $f(u)$ не определено.*

Доказательство. Пусть $\mathcal{M}$ — машина Тьюринга, вычисляющая функцию f в сильном смысле. Построим машину $\mathcal{N}$, вычисляющую функцию f в сильном смысле и не останавливающуюся на тех входах $u \in \Sigma^*$, для которых $\mathcal{M}$ не дает результата. Мы ограничимся лишь описанием работы машины $\mathcal{N}$, а программу для $\mathcal{N}$ читатель сможет написать самостоятельно. По условию, работа машины $\mathcal{N}$ на входе u должна отличаться от работы машины $\mathcal{M}$ на входе u в следующих двух случаях:

1) если машина $\mathcal{M}$ при работе на входе u пытается выйти за край ленты;

2) если машина $\mathcal{M}$ при работе на входе u остановилась в заключительном состоянии, но при этом заключительная конфигурация не может быть записана в виде слова $q_0 0v$ ни для какого слова $v \in \Delta^*$.

Машину $\mathcal{N}$ мы устроим следующим образом. Она «запускает» машину $\mathcal{M}$, и если в своем вычислении $\mathcal{M}$ пытается выйти за край ленты, то $\mathcal{N}$ зацикливается. Если машина $\mathcal{M}$ не останавливается, то тем самым и машина $\mathcal{N}$ не останавливается. Если же $\mathcal{M}$ остановится, то после окончания работы машины $\mathcal{M}$ машина $\mathcal{N}$ находит место на ленте, начиная с которого написаны одни нули, и выясняет, имеет ли заключительная конфигурация вид $q_0 0v$, где $v \in \Delta^*$. Однако, вообще говоря, невозможно определить, с какой ячейки начинаются одни нули, поскольку машина $\mathcal{M}$ могла побывать в сколь угодно далеких ячейках. Чтобы решить эту проблему, мы изменим машину $\mathcal{M}$, заставив ее помечать все ячейки, в которых она побывала, и будем вместо $\mathcal{M}$ использовать эту новую машину.

Более подробно, работа машины $\mathcal{N}$ происходит в три этапа.

1. Машина $\mathcal{N}$ пишет вместо самого левого нуля специальный символ #, затем сдвигает входное слово на одну ячейку вправо, записав в освободившуюся ячейку символ 0.

2. Машина $\mathcal{N}$ запускает новую машину $\widetilde{\mathcal{M}}$. Машина $\widetilde{\mathcal{M}}$ — это, по определению, немного измененная машина $\mathcal{M}$. Именно, работа

машины $\widetilde{\mathcal{M}}$ отличается от работы машины $\mathcal{M}$ тем, что она пишет новый специальный символ o, а при чтении воспринимает его так же, как и нуль. Это нужно для того, чтобы после окончания работы машины $\widetilde{\mathcal{M}}$ можно было выяснить, в каких ячейках побывала бы машина $\mathcal{M}$ при работе на входе u. Кроме того, как только машина $\widetilde{\mathcal{M}}$ видит символ #, она зацикливается. Формально, программа машины $\widetilde{\mathcal{M}}$ получается из программы машины $\mathcal{M}$ добавлением для каждой команды вида $q0 \to ar$, $q0 \to aLr$ или $q0 \to aRr$ соответственно команды $qo \to ar$, $qo \to aLr$ или $qo \to aRr$, затем заменой нуля в правой части любой команды на o и добавлением новых команд $q\# \to \#q$ для всех состояний q машины $\mathcal{M}$.

Про работу машины $\widetilde{\mathcal{M}}$ можно утверждать следующее. Если $\mathcal{M}$ во время работы на входе u пытается выйти за край ленты, то $\widetilde{\mathcal{M}}$ на том же входе работает бесконечно. Если $\mathcal{M}$ на входе u работает бесконечно долго, то и $\widetilde{\mathcal{M}}$ на входе u работает бесконечно долго. Если $\mathcal{M}$ останавливается на входе u в заключительном состоянии, и v — слово, записанное на ленте слева направо от крайней левой ячейки до крайней правой из посещенных машиной $\mathcal{M}$ ячеек, то $\widetilde{\mathcal{M}}$ также останавливается на входе u в том же состоянии и в той же ячейке, а на ленте записано слово $\widetilde{v}$, полученное из слова v заменой всех нулей на o.

3. Теперь $\mathcal{N}$ проверяет, имеет ли текущая конфигурация вид $\#qovo\ldots o$, где $v \in \Delta^*$, а q — заключительное состояние машины $\mathcal{M}$. Если имеет, то $\mathcal{M}$ дала результат на слове u; в этом случае $\mathcal{N}$ заменяет все символы o на нули, сдвигает слово v на одну ячейку влево и заменяет # на нуль. Если же конфигурация не имеет такого вида, то $\mathcal{N}$ зацикливается.

Теорема доказана.

Теорема 19. *Каковы бы ни были алфавиты Σ и Δ такие, что $0 \notin \Sigma$, $0 \notin \Delta$, и частичная функция f из Σ^* в Δ^*, функция f вычислима по Тьюрингу в сильном смысле тогда и только тогда, когда f вычислима по Тьюрингу в слабом смысле.*

Доказательство. Пусть функция f из Σ^* в Δ^* вычислима по Тьюрингу в сильном смысле. В силу теоремы 18 существует машина Тьюринга $\mathcal{N}$, вычисляющая функцию f в сильном смысле, которая работает бесконечно долго на всех входах $u \in \Sigma^*$, для которых значение $f(u)$ не определено. Пусть $\mathcal{N}$ имеет состояния $q_0, q_1, \ldots, q_n$. Построим машину $\mathcal{N}'$, вычисляющую функцию f в слабом смысле. Машина $\mathcal{N}'$ будет иметь тот же алфавит, что и машина $\mathcal{N}$, и состояния $q_0, q_1, \ldots, q_n, q_{n+1}$. Программа машины $\mathcal{N}'$ строится следующим

образом: в программе машины $\mathcal{N}$ во всех командах состояние q_0 заменяется на состояние q_{n+1}, и к полученной программе добавляется команда $q_{n+1}0 \to 0Rq_0$.

Покажем, что машина $\mathcal{N}'$ вычисляет функцию f в слабом смысле. Если значение $f(u)$ не определено, то машина $\mathcal{N}$ на входе u зацикливается, а тогда, очевидно, машина $\mathcal{N}'$ также зацикливается. Если значение $f(u)$ определено и равно пустому слову, то машина $\mathcal{N}$ на входе u завершает работу в конфигурации $q_0 0$, а тогда, очевидно, машина $\mathcal{N}'$ на входе u завершает работу в конфигурации $0q_0 0$, т.е. пустое слово является результатом вычисления в слабом смысле. Наконец, если значение $f(u)$ определено и равно непустому слову $v \in \Delta^*$, то машина $\mathcal{N}$ на входе u завершает работу в конфигурации $q_0 0v0\dots0$, а тогда, очевидно, машина $\mathcal{N}'$ на входе u завершает работу в конфигурации $0q_0 v0\dots0$, т.е. слово v является результатом вычисления в слабом смысле.

Докажем теперь, что если функция f из Σ^* в Δ^* вычислима по Тьюрингу в слабом смысле, то она вычислима и в сильном смысле. Пусть машина Тьюринга $\mathcal{M}$ вычисляет функцию f в слабом смысле. Подобно тому, как это было сделано в доказательстве теоремы 18, построим машину $\widetilde{\mathcal{M}}$, которая вместо самого левого нуля пишет символ #, сдвигает входное слово на одну ячейку вправо, записав в освободившуюся ячейку нуль, и затем работает, как $\mathcal{M}$, за тем лишь исключением, что вместо нуля она пишет символ o, который при чтении воспринимает так же, как и нуль, а увидев символ #, машина $\widetilde{\mathcal{M}}$ зацикливается.

Таким образом, если $\mathcal{M}$ во время работы на входе u пытается выйти за край ленты, то $\widetilde{\mathcal{M}}$ на том же входе работает бесконечно; если $\mathcal{M}$ на входе u работает бесконечно долго, то и $\widetilde{\mathcal{M}}$ на входе u работает бесконечно долго; если $\mathcal{M}$ останавливается на входе u в заключительном состоянии, и $\#v$ — слово, записанное на ленте от крайней левой ячейки до крайней правой из посещенных машиной $\mathcal{M}$ ячеек, то $\widetilde{\mathcal{M}}$ также останавливается на входе u в том же состоянии и в той же ячейке, а на ленте записано слово $\#\widetilde{v}$, полученное из слова v заменой всех нулей на o.

Построим теперь машину $\mathcal{N}$, которая сначала работает, как $\widetilde{\mathcal{M}}$, а в случае остановки последней проверяет, принадлежит ли обозреваемый символ алфавиту Δ. Если нет, то машина $\mathcal{N}$ стирает с ленты все символы, заменяя их на нули, и останавливается в крайней левой ячейке (где был написан символ #). Если же обозреваемый символ принадлежит алфавиту Δ, машина $\mathcal{N}$ двигается по ленте вправо, не меняя содержимое ячеек, пока не закончатся символы

из алфавита Δ, затем, продолжая движение вправо, стирает все остальные символы, пока не встретится нуль. После этого машина двигается влево, пока не начнутся символы из алфавита Δ. Не меняя их, машина продолжает движение влево, пока не закончатся символы из алфавита Δ, затем, продолжая движение влево, стирает все остальные символы, пока не встретится символ $\#$. После этого машина сдвигает оставшееся на ленте непустое слово в алфавите Δ влево, записывая его буква за буквой справа от ячейки, содержащей символ $\#$. Затем машина возвращается в ячейку, содержащую символ $\#$, заменяет его на нуль и останавливается в этой ячейке в состоянии q_0. Очевидно, что так построенная машина вычисляет функцию f в сильном смысле.

Теорема доказана.

Будем говорить, что функция f вычислима по Тьюрингу, если она вычислима по Тьюрингу в сильном или слабом смысле, что в силу теоремы 19 одно и то же. Обычно, как в рассмотренном примере 2, программа для вычисления функции в слабом смысле несколько проще, чем программа для вычисления той же функции в сильном смысле. Однако в теоретических конструкциях программа для вычисления функции в сильном смысле предпочтительнее, так как она представляет результат вычисления в виде, пригодном для применения к нему другой программы. Это факт используется, например, при доказательстве следующей теоремы.

Теорема 20. *Если функция f из Σ^* в Δ^* и функция g из Δ^* в Γ^* вычислимы по Тьюрингу, то их композиция $f \circ g$ вычислима по Тьюрингу.*

Мы не будем доказывать эту теорему, поскольку ее доказательство не использует новых идей и проводится путем непосредственного описания процедуры получения программы машины Тьюринга для вычисления функции $f \circ g$ в сильном смысле из программ машин Тьюринга, вычисляющих в сильном смысле функции f и g.

Общее понятие функции, вычислимой по Тьюрингу, позволяет следующим образом определить вычислимые по Тьюрингу функции натурального аргумента. Отождествим натуральные числа и слова в алфавите $\{|\}$. А именно, пусть пустое слово обозначает натуральное число 0, слово $|$ обозначает число 1, слово $||$ — число 2, и вообще, слово $|\ldots|$, состоящее из n букв $|$, обозначает число n. Таким образом, вычислимая по Тьюрингу частичная функция из $\mathbb{N}$ в $\mathbb{N}$ — это вычислимая по Тьюрингу частичная функция из $\{|\}^*$ в $\{|\}^*$.

Наконец, определим понятие вычислимой функции из $\Sigma^* \times \Gamma^*$ в Δ^* для произвольных алфавитов Σ, Γ, Δ. Пусть символ $\#$ не содержится в алфавитах Σ и Γ. Функцию f из $\Sigma^* \times \Gamma^*$ в Δ^* будем считать вычислимой по Тьюрингу, если вычислима функция $\overline{f}$ из $\Sigma^* \cup \Gamma^* \cup \{\#\}$ в Δ^*, определенная следующим образом:

$$\overline{f}(w) \simeq \begin{cases} f(u,v), \text{ если } w = u\#v, \\ \text{не определено, если } w \text{ не имеет такого вида.} \end{cases}$$

Таким образом, машина Тьюринга, вычисляющая функцию f, должна на входе $u\#v$ дать результат $f(u,v)$. Аналогично определяется вычислимость по Тьюрингу функции из $\Sigma_1^* \times \ldots \times \Sigma_n^*$ в Δ^*.

Упражнения.

1. Доказать, что по программе машины Тьюринга нельзя определить, вычисляет ли она всюду определенную функцию из $\mathbb{N}$ в $\mathbb{N}$.

2. Доказать, что по программе машины Тьюринга нельзя определить, вычисляет ли она где-то определенную функцию из $\mathbb{N}$ в $\mathbb{N}$.

3. Доказать, что по программе машины Тьюринга нельзя определить, останавливается ли она, начиная работу с пустой лентой.

§ 8. Универсальная вычислимая по Тьюрингу функция

Пусть Σ, Δ — два алфавита. Мы собираемся для каждой машины Тьюринга, ленточный алфавит которой включает Σ и Δ, записать ее программу как слово в некотором алфавите Б. Положим Б $= \{1, q, \to, R, L, *\}$. Каждую букву алфавитов Σ и Δ закодируем последовательностью единиц. Например, если $\Sigma = \{a, b\}$, $\Delta = \{c, d\}$, то закодируем $a \leftrightarrow 1$, $b \leftrightarrow 11$, $c \leftrightarrow 111$, $d \leftrightarrow 1111$. Зафиксируем любое такое кодирование букв Σ и Δ. Пусть $\mathcal{M}$ — произвольная машина Тьюринга, алфавит которой включает Σ и Δ. Закодируем каждое состояние $\mathcal{M}$ последовательностью букв q: состояние q_0 последовательностью q, состояние q_1 — qq и т. д. Каждый символ ленточного алфавита $\mathcal{M}$, не содержащийся в $\Sigma \cup \Delta$, закодируем любым способом последовательностью единиц, которая не была использована при кодировании $\Sigma \cup \Delta$. Каждой команде $\mathcal{M}$ сопоставим слово, составленное из кодов левой и правой частей команд, разделенных знаком $\to$. Программе $\mathcal{M}$ сопоставим слово, полученное из слов, сопоставленных ее командам, записанных в любом порядке и разделенных символом $*$. Будем называть это слово *записью программы* $\mathcal{M}$. Например, запись программы машины из примера 2

имеет вид

$$qq111 \to 1111Rqqq * qqq1 \to 111Rqqqq * qqq11 \to R\ldots.$$

Здесь мы закодировали $a \leftrightarrow 1$, $b \leftrightarrow 11$, $0 \leftrightarrow 111$, $\sharp \leftrightarrow 1111$.

Определим функцию F из $Б^* \times \Sigma^*$ в Δ^* следующим образом. $(F(P, u) = v) \leftrightarrow$ (P является записью программы некоторой машины $\mathcal{M}$, дающей на выходе u результат v).

Теорема 21 (теорема об универсальной вычислимой по Тьюрингу функции).

1) *Функция F вычислима по Тьюрингу.*

2) *Функция F универсальна для вычислимых по Тьюрингу функций из Σ^* в Δ^* в следующем смысле: для любой вычислимой по Тьюрингу функции f из Σ^* в Δ^* существует слово $P \in Б^*$, для которого $f(u) \simeq F(P, u)$ для всех $u \in \Sigma^*$.*

Вторая часть теоремы очевидна. Доказательство первой части требует аккуратного построения машины Тьюринга, вычисляющей F. Это построение мы не приводим.

В дальнейшем ограничимся для простоты однобуквенными алфавитами $\Sigma = \{|\}$, $\Delta = \{|\}$. Напомним, что множество всех слов в алфавите $\{|\}$ мы отождествили с множеством натуральных чисел.

Теорема 22 (теорема о неразрешимости проблемы остановки машины Тьюринга). *Функция $Ост : Б^* \times \mathbb{N} \to \mathbb{N}$, определенная равенством*

$$Ост(P, n) = \begin{cases} 1, & \text{если } P \text{ — запись программы машины Тьюринга, останавливающейся на входе } n; \\ 0, & \text{если } P \text{ не является записью программы никакой машины или машина с записью программы } P \text{ не останавливается на входе } n, \end{cases}$$

не является вычислимой по Тьюрингу.

Доказательство от противного. Предположим, что функция $Ост$ вычислима по Тьюрингу.

Перенумеруем все слова в алфавите Б в порядке возрастания длины, а при одной длине — в лексикографическом порядке; обозначим n-е слово P_n. Машину с записью программы P_n будем обозначать $\mathcal{M}_n$. Нетрудно доказать, что функция $f : \mathbb{N} \to Б^*$, переводящая n в P_n, вычислима по Тьюрингу. Тогда и функция

$Ост(P_n, m)$ двух натуральных аргументов n и m вычислима по Тьюрингу. Пусть $\mathcal{M}_{n_0}$ — машина Тьюринга, которая на входе $m \in \mathbb{N}$ работает так: вычисляет $Ост(P_m, m)$ и если $Ост(P_m, m) = 1$, то зацикливается, а иначе останавливается. Тогда для любой машины $\mathcal{M}_m$ следующие два утверждения равносильны:

(1) $\mathcal{M}_m$ останавливается на входе m;

(2) машина $\mathcal{M}_{n_0}$ не останавливается на входе m.

Взяв $m = n_0$, мы получим противоречие.

§ 9. Тезис Чёрча

Нетрудно проверить, что вычислимые по Тьюрингу функции из Σ^* в Σ^* удовлетворяют всем свойствам вычислимых функций, сформулированным в §§ 1–6 или неявно использованым там. Точнее, если ограничиться ансамблями вида Σ^* (среди них есть и $\mathbb{N}$, так как мы отождествили $\{|\}^*$ и $\mathbb{N}$) и заменить всюду слова «вычислимая функция» на «вычислимая по Тьюрингу функция», то все теоремы §§ 1–6 останутся справедливыми. Возникает предположение о совпадении класса вычислимых по Тьюрингу функций и класса функций, вычислимых в интуитивном смысле (использованном в §§ 1–6). Это предположение носит название *тезиса Чёрча.* Поскольку очевидно, что всякая вычислимая по Тьюрингу функция вычислима в интуитивном смысле, тезис Чёрча имеет следующий вид:

> *для любой функции $f \in Com(\Sigma^*, \Sigma^*)$ существует алфавит $\Gamma \supseteq \Sigma$ и машина Тьюринга с алфавитом Γ, которая вычисляет f.*

Тезис Чёрча невозможно ни доказать, ни опровергнуть, так как понятие вычислимой функции не определено формально. Все до сих пор предложенные формальные уточнения понятия вычислимости не вывели за класс вычислимых по Тьюрингу функций. Это служит некоторым подтверждением тезиса Чёрча. Кроме того, до сих пор никому не удавалось привести пример (или доказать существование такового) вычислимой, но не вычислимой по Тьюрингу функции.

Если верить в тезис Чёрча, то первую часть теоремы об универсальной вычислимой по Тьюрингу функции доказывать не нужно: ведь функция F вычислима; более того, для установления вычислимости по Тьюрингу любой функции достаточно предъявить неформальный алгоритм, вычисляющий ее.

СПИСОК РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ

1. Верещагин Н.К., Шень А. Вычислимые функции. — М.: МЦНМО, 1999. – 176 с.

2. Верещагин Н.К., Шень А. Языки и исчисления. — М.: МЦНМО, 2000. – 288 с.

3. Гиндикин С.Г. Алгебра логики в задачах. — М.: Наука, 1972. — 288 с.

4. Ершов Ю.Л., Палютин Е.А. Математическая логика. — М.: Наука, 1987. — 336 с.

5. Катленд Н. Вычислимость. Введение в теорию рекурсивных функций. — М.: Мир, 1985. — 256 с.

6. Клини С.К. Математическая логика. — М.: Мир, 1973. — 480 с.

7. Колмогоров А.Н., Драгалин А.Г. Введение в математическую логику. — М.: Изд-во моск. ун-та, 1982. — 120 с.

8. Колмогоров А.Н., Драгалин А.Г. Математическая логика. Дополнительные главы. — М.: Изд-во Моск. ун-та, 1984. — 119 с.

9. Лавров И.А., Максимова Л.Л. Задачи по теории множеств, математической логики и теории алгоритмов. — М.: ФИЗМАТЛИТ, 2002. — 256 с.

10. Марков А.А. Элементы математической логики. — М.: Изд-во Моск. ун-та, 1984. — 80 с.

11. Мендельсон Э. Введение в математическую логику. — М.: Наука, 1971. — 320 с.

12. Новиков П.С. Элементы математической логики. — М.: Наука, 1971. — 400 с.

13. Столл Р.Р. Множество. Логика. Аксиоматические теории. — М.: Просвещение, 1968. — 231 с.

14. Успенский В.А. Лекции о вычислимых функциях. — М.: Физматгиз, 1960. — 492 с.

15. Чёрч А. Введение в математическую логику. — М.: ИЛ, 1960. — 484 с.

ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

Учебное издание

УСПЕНСКИЙ Владимир Андреевич
ВЕРЕЩАГИН Николай Константинович
ПЛИСКО Валерий Егорович

ВВОДНЫЙ КУРС МАТЕМАТИЧЕСКОЙ ЛОГИКИ

Редактор *И.Л. Легостаева*
Оригинал-макет: *И.Л. Панкратьева*
Оформление переплета: *А.А. Логунов*

ЛР № 071930 от 06.07.99. Подписано в печать 04.12.03.
Формат 60×90/16. Бумага офсетная. Печать офсетная.
Усл. печ. л. 8. Уч.-изд. л. 8. Заказ №

Издательская фирма «Физико-математическая литература»
МАИК «Наука/Интерпериодика»
117997, Москва, ул. Профсоюзная, 90
E-mail: fizmat@maik.ru

Отпечатано с готовых диапозитивов в ПФ «Полиграфист»
160001, г. Вологда, ул. Челюскинцев, 3
Тел.: (8172) 72-55-31, 72-61-75, факс: (8172) 72-60-72
E-mail: form.pfp@votel.ru   http://www.vologda/~pfpv

ISBN 5-9221-0278-8

